(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107147639 A
(43)申请公布日 2017.09.08

(21)申请号 201710316301.9

(22)申请日 2017.05.08

(71)申请人 国家电网公司
地址 100031 北京市西城区西长安街86号
申请人 南京南瑞集团公司
南京南瑞信息通信科技有限公司
国网福建省电力有限公司信息通信分公司

(72)发明人 姜帆 于晓文 刘莹 金倩倩 郭靓 李炜键 贾雪 俞皓 张路煜 屠正伟 张丹 张骞 刘强 栾国强 林苏蓉 傅慧斌 杨业平

(74)专利代理机构 南京纵横知识产权代理有限公司 32224
代理人 姚兰兰 董建林

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/57(2013.01)
G06F 21/55(2013.01)
G06F 17/30(2006.01)

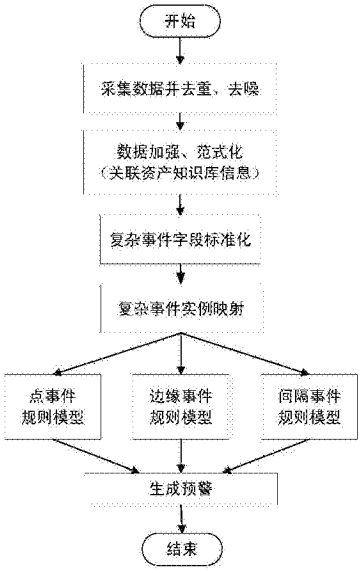
权利要求书3页 说明书7页 附图2页

(54)发明名称

一种基于复杂事件处理的实时安全预警方法

(57)摘要

本发明公开了一种基于复杂事件处理的实时安全预警方法，具体包括以下几个步骤：(1)利用范式化引擎将采集到的安全数据进行日志字段分割，并依据字段的要求对字段进行规范化，按照期望输出的字段，关联知识库信息；(2)利用数据流语义分析引擎，依据将要作为场景建模的复杂事件实例，进行数据上下文分析，依据标准化的分析字段模板，分析映射流数据；(3)利用安全分析模型计算引擎，在分析规则计算模块中，基于点事件、边缘事件、间隔事件进行按场景分析，生成预警事件。本发明通过可配置的范式化规则、语义识别规则、安全分析规则实现原始日志数据的多角度关联分析，及时发现未知威胁并进行预警。



CN 107147639 A

1.一种基于复杂事件处理的实时安全预警方法，其特征在于，具体包括以下几个步骤：

(1)利用范式化引擎将采集到的安全数据进行日志字段分割，并依据字段的要求对字段进行规范，按照期望输出的字段，关联知识库信息；所述范式化引擎实现日志数据的匹配、去重、去噪、关联静态数据；范式化引擎依照数据处理的先后次序包括去重去噪模块、数据加强模块、数据格式化模块；

(2)利用数据流语义分析引擎，将要作为场景建模的复杂事件实例，进行数据上下文分析，依据标准化的分析字段模板，分析映射流数据；所述数据流语义分析引擎实现范式化后数据的事件语义识别，通过关联预设语义识别和提取规则，将范式化数据分解成符合分析模型识别的事件数据分片；数据流语义分析引擎依照事件处理的先后次序包括复杂事件字段标准化模块和复杂事件实例映射模块；

(3)利用安全分析模型计算引擎，在分析规则计算模块中，基于点事件、边缘事件、间隔事件进行按场景分析，生成预警事件；所述安全分析模型计算引擎实现实时分析模型计算及安全预警输出，通过复杂事件处理逻辑，在内存中进行符合语义数据的计算及标准化实时预警的生成；安全分析模型计算引擎依照安全场景建模并生成预警的先后次序包括分析规则计算模块和标准化预警输出模块。

2.根据权利要求1所述的基于复杂事件处理的实时安全预警方法，其特征在于，步骤(1)中，所述范式化引擎的处理过程如下：

(1-1)范式化引擎启动，加载范式化引擎中用于数据处理的规则，并转化为复杂事件处理CEP查询；

(1-2)所述去重去噪模块将CEP查询解析成日志分隔符解析事件处理语句，针对时间字段的去噪处理语句和字段去重处理语句，基于实时数据流执行CEP查询，完成去重去噪；

(1-3)所述数据加强模块将CEP查询解析成关联数据查询语句，利用CEP查询联合资产数据库表和IP位置数据库表，对经过去重、去噪的数据流进行加强操作；

(1-4)所述数据格式化模块将CEP查询解析成日志标准化字段处理语句，然后通过执行CEP查询对加强后的数据流进行数据格式范式化。

3.根据权利要求1所述的基于复杂事件处理的实时安全预警方法，其特征在于，步骤(2)中，所述数据流语义分析引擎的处理过程如下：

(2-1)数据流语义分析引擎启动，加载数据流语义分析引擎中用于数据流语义分析的规则，并转化为CEP查询；

(2-2)所述复杂事件字段标准化模块依据标准复杂事件模板将CEP查询解析成复杂事件标准化查询语句，通过执行CEP查询，依据实时数据流类型提取关联的事件模板；

(2-3)所述复杂事件实例映射模块基于事件模板将CEP查询解析成事件实例提取处理语句，通过在实时数据流中执行该查询，将数据流解析、转化为符合不同类型事件模板的实例。

4.根据权利要求1所述的基于复杂事件处理的实时安全预警方法，其特征在于，步骤(3)中，所述安全分析模型计算引擎的处理过程如下：

(3-1)安全分析模型计算引擎启动，加载安全分析模型计算引擎中用于安全事件分析、预警生成的规则，并转化为CEP查询；

(3-2)分析规则计算模块将CEP查询解析成用于分析数据处理语句及预警事件窗处理

语句，依据预置或自定义的规则，对数据流语义分析引擎处理过的数据流进行数据计算；

(3-3)所述标准化预警输出模块将CEP查询解析成预警输出标准化处理语句，对经过规则计算和分析的数据流进行标准化解析，生成预警输出。

5.根据权利要求1所述的基于复杂事件处理的实时安全预警方法，其特征在于，所述范式化引擎运行的具体步骤为：

(4-1)字段正则匹配、拆分、去重、去噪

对日志数据类型进行匹配识别，将各类日志已拆分的字段依据规范化标准进行处理，对发送过来有数字有英文表示法的数据处理后合并，最终统一标准化成标准时间戳格式；将不同厂商的同类型日志进行合并，并使用md5值判定的方法进行日志的去重，即将数据各字段联合计算md5值，如果值相同即为重复；将日志中的字段名以规范好的字段约束；

(4-2)由知识库及已知日志字段推导未知字段

使用类SQL语句联系已有知识库数据，进行关联分析，按序分步推导出相关字段，需要关联分析推导出的字段有：源或目的地址的位置信息、资产信息；每种类型标准化后的字段加上加强后需要的字段新增字段形成范式化后最终字段集合，需要发送到数据检索引擎的字段置为输出项，其他备用字段置为非输出项；

(4-3)联合推导形成范式化最终字段

依据数据格式化模块记录的类SQL及日志字段之间的关联，将不同日志加强分析后的字段加入到对应日志的字段集合中。

6.根据权利要求1所述的基于复杂事件处理的实时安全预警方法，其特征在于，所述数据流语义分析引擎运行的具体步骤为：

(5-1)复杂事件字段标准化

所述复杂事件字段标准化模块中，存储着范式化后日志数据的模型号、类型、字段名称，每一行数据是一个规则元组，是后续复杂事件提取的规则；

(5-2)复杂事件字段提取

复杂事件由连续的、流动的数据组成，这些数据在所述复杂事件实例映射模块中，依据标准复杂事件字段模块的规则，映射成一条条实例。

7.根据权利要求1所述的基于复杂事件处理的实时安全预警方法，其特征在于，所述安全分析模型计算引擎运行的具体步骤为：

(6-1)场景建模，生成预警事件

所述分析规则计算模块将经过复杂事件字段提取模块提取的复杂事件，通过Esper技术使用EPL语法进行关联场景分析；分析规则计算模块还包括场景建模规则表，这些表是通过预置或者人工生成的方式定义的；

(6-2)标准化预警格式建立

标准化预警格式建立是由标准化预警输出模板进行预先建立的，格式是预置好的，所有的预警输出都是一致的，包括预警事件的名称、预警产生的原因字段，预警产生时间。

8.根据权利要求1所述的基于复杂事件处理的实时安全预警方法，其特征在于，所述点事件、边缘事件、间隔事件各定义如下：

a)点事件

在某一时刻或者基于某一条复杂事件进行分析推导出的预警事件；

b)边缘事件

只对某一同类型事件进行的分析推导出的预警事件；

c)间隔事件

对复杂事件中的某几类事件的分析推导出的预警事件，间隔事件是复杂事件中组合最多的一种情况，不局限于一类日志。

一种基于复杂事件处理的实时安全预警方法

技术领域

[0001] 本发明涉及一种基于复杂事件处理的实时安全预警方法，属于大数据的信息安全监测预警技术领域。

背景技术

[0002] 企业在发展的过程中网络架构不断调整变化，层出不穷的网络安全问题，加之企业中用户的安全意识提高，企业内部信息安全的预防性控制决策分析成为一个重要课题。传统的安全预警方法针对单一的威胁，定义指定的威胁分析预警规则，其规则是固定、单一和分离的，随着攻击手段的发展，传统的方式已经不能满足联合的多步骤的威胁预警需求，且传统的安全预警方法大部分基于阈值分析，是将分析对象确定在某一固定范围内，事件处理较保守，不能实时全面地基于复杂事件对海量数据进行处理和预警。

[0003] 综上所述，对于不同环境、不同厂商中的异构源数据，使用传统的安全预警处理方法只针对单一的、确定的、严重的安全日志。并且传统的安全预警处理方法没有形成一套统一的复杂事件处理规则完成数据范式化、语义转换、规则分析及预警生成，不利于多步骤的安全事件预警，容易导致事件漏报，对新增的预警类型及分析规则的拓展能力也较弱。

发明内容

[0004] 针对现有技术存在的不足，本发明目的是提供一种基于复杂事件处理的实时安全预警方法，通过可配置的范式化规则、语义识别规则、安全分析规则实现原始日志数据的多角度关联分析，及时发现未知威胁并进行预警。

[0005] 为了实现上述目的，本发明是通过如下的技术方案来实现：

[0006] 本发明一种基于复杂事件处理的实时安全预警方法，具体包括以下几个步骤：

[0007] (1)利用范式化引擎(范式化引擎：一种通过分解原始日志数据中字段，并处理字段之间关系来消除不适合的数据依赖的数据处理引擎)将采集到的安全数据进行日志字段分割，并依据字段的要求对字段进行规范，按照期望输出的字段，关联知识库信息；所述范式化引擎(每类引擎的名称是依据具体要实现的任务抽取出来的概括性名称。引擎里面包括的模块是依据事件(数据)处理的先后次序及任务的进一步划分提炼出来的模块名称)实现日志数据的匹配、去重、去噪、关联静态数据；范式化引擎依照数据处理的先后次序包括去重去噪模块、数据加强模块、数据格式化模块；

[0008] (2)利用数据流语义分析引擎(数据流语义分析引擎：通过对实际场景的复杂事件的上下文、场景分析，消除不符合逻辑的冗余数据的数据分析引擎)，依据将要作为场景建模的复杂事件实例，进行数据上下文分析，依据标准化的分析字段模板，分析映射流数据；所述数据流语义分析引擎实现范式化后数据的事件语义识别，通过关联预设语义识别和提取规则，将范式化数据分解成符合分析模型识别的事件数据分片；数据流语义分析引擎依照事件处理的先后次序包括复杂事件字段标准化模块和复杂事件实例映射模块；

[0009] (3)利用安全分析模型计算引擎(安全分析模型计算引擎：是一种通过对安全事件

进行抽象、建模、分析、计算之后生成预警的复杂事件计算引擎)，在分析规则计算模块中，基于点事件、边缘事件、间隔事件进行按场景分析，生成预警事件；所述安全分析模型计算引擎实现实时分析模型计算及安全预警输出，通过复杂事件处理逻辑，在内存中进行符合语义数据的计算及标准化实时预警的生成；安全分析模型计算引擎依照安全场景建模并生成预警的先后次序包括分析规则计算模块和标准化预警输出模块。

[0010] 步骤(1)中，所述范式化引擎的处理过程如下：

[0011] (1-1)范式化引擎启动，加载范式化引擎中用于数据处理的规则，并转化为复杂事件处理CEP查询；

[0012] (1-2)所述去重去噪模块将CEP查询解析成日志分隔符解析事件处理语句，针对时间字段的去噪处理语句和字段去重处理语句，基于实时数据流执行CEP查询，完成去重去噪；

[0013] (1-3)所述数据加强模块将CEP查询解析成关联数据查询语句，利用CEP查询联合资产数据库表和IP位置数据库表，对经过去重、去噪的数据流进行加强操作；

[0014] (1-4)所述数据格式化模块将CEP查询解析成日志标准化字段处理语句，然后通过执行CEP查询对加强后的数据流进行数据格式范式化。

[0015] 步骤(2)中，所述数据流语义分析引擎的处理过程如下：

[0016] (2-1)数据流语义分析引擎启动，加载数据流语义分析引擎中用于数据流语义分析的规则，并转化为CEP查询；

[0017] (2-2)所述复杂事件字段标准化模块依据标准复杂事件模板将CEP查询解析成复杂事件标准化查询语句，通过执行CEP查询，依据实时数据流类型提取关联的事件模板；

[0018] (2-3)所述复杂事件实例映射模块基于事件模板将CEP查询解析成事件实例提取处理语句，通过在实时数据流中执行该查询，将数据流解析、转化为符合不同类型事件模板的实例。

[0019] 步骤(3)中，所述安全分析模型计算引擎的处理过程如下：

[0020] (3-1)安全分析模型计算引擎启动，加载安全分析模型计算引擎中用于安全事件分析、预警生成的规则，并转化为CEP查询；

[0021] (3-2)分析规则计算模块将CEP查询解析成用于分析数据处理语句及预警事件窗处理语句，依据预置或自定义的规则，对数据流语义分析引擎处理过的数据流进行数据计算；

[0022] (3-3)所述标准化预警输出模块将CEP查询解析成预警输出标准化处理语句，对经过规则计算和分析的数据流进行标准化解析，生成预警输出。

[0023] 上述范式化引擎运行的具体步骤为：

[0024] (4-1)字段正则匹配、拆分、去重、去噪

[0025] 对日志数据类型进行匹配识别，将各类日志已拆分的字段依据规范化标准进行处理，对发送过来有数字有英文表示法的数据处理后合并，最终统一标准化成标准时间戳格式；将不同厂商的同类型日志进行合并，并使用md5值判定的方法进行日志的去重，即将数据各字段联合计算md5值，如果值相同即为重复；将日志中的字段名以规范好的字段约束；

[0026] (4-2)由知识库及已知日志字段推导未知字段

[0027] 使用类SQL语句联系已有知识库数据，进行关联分析，按序分步推导出相关字段，

需要关联分析推导出的字段有:源或目的地址的位置信息、资产信息;每种类型标准化后的字段加上加强后需要的字段新增字段形成范式化后最终字段集合,需要发送到数据检索引擎的字段置为输出项,其他备用字段置为非输出项;

[0028] (4-3)联合推导形成范式化最终字段

[0029] 依据数据格式化模块记录的类SQL及日志字段之间的关联,将不同日志加强分析后的字段加入到对应日志的字段集合中。

[0030] 上述数据流语义分析引擎运行的具体步骤为:

[0031] (5-1)复杂事件字段标准化

[0032] 所述复杂事件字段标准化模块中,存储着范式化后日志数据的模型号、类型、字段名称,每一行数据是一个规则元组,是后续复杂事件提取的规则;

[0033] (5-2)复杂事件字段提取

[0034] 复杂事件由连续的、流动的数据组成,这些数据在所述复杂事件实例映射模块中,依据标准复杂事件字段模块的规则,映射成一条条实例。

[0035] 上述安全分析模型计算引擎运行的具体步骤为:

[0036] (6-1)场景建模,生成预警事件

[0037] 所述分析规则计算模块将经过复杂事件字段提取模块提取的复杂事件,通过Esper技术使用EPL语法进行关联场景分析;分析规则计算模块还包括场景建模规则表,这些表是通过预置或者人工生成的方式定义的;

[0038] (6-2)标准化预警格式建立

[0039] 标准化预警格式建立是由标准化预警输出模板进行预先建立的,格式是预置好的,所有的预警输出都是一致的,包括预警事件的名称、预警产生的原因字段,预警产生时间。

[0040] 上述点事件、边缘事件、间隔事件各定义如下:

[0041] a)点事件

[0042] 在某一时刻或者基于某一条复杂事件进行分析推导出的预警事件;

[0043] b)边缘事件

[0044] 只对某一同类型事件进行的分析推导出的预警事件;

[0045] c)间隔事件

[0046] 对复杂事件中的某几类事件的分析推导出的预警事件,间隔事件是复杂事件中组合最多的一种情况,不局限于一类日志。

[0047] 本发明所达到的有益效果:本发明通过对采集到的安全日志数据进行去重去噪、范式化和数据流语义分析、场景建模分析,从不同角度进行分析,最终生成安全预警事件;在传统的预警事件生成基础上,提高了场景分析的灵活性,并使用流式处理技术,实时地对连续的安全日志进行分析预警。

附图说明

[0048] 图1为本发明的主引擎、从模块协作架构图;

[0049] 图2为本发明的实时安全预警方法处理流程图;

[0050] 图3为本发明的各引擎结构图。

具体实施方式

[0051] 为使本发明实现的技术手段、创作特征、达成目的与功效易于明白了解，下面结合具体实施方式，进一步阐述本发明。

[0052] 参见图1至图3，本发明的一种基于复杂事件处理的实时安全预警方法，包括以下几个步骤：

[0053] (1)采集到的数据实时进入安全预警框架，进行去重去噪，动态数据(实时数据)关联静态数据(资产数据)进行范式化；

[0054] (2)范式化后的数据按照语义上下文进行提取、映射为复杂事件字段，为预警生成做准备；

[0055] (3)结合场景规则建立模型，对数据进行分析，生成实时预警事件。

[0056] 本发明在使用CEP及Kafka、Storm和Esper等开源技术架构的基础上，基于复杂事件，设计了实时安全预警的方法，将静态数据(资产数据)与动态安全数据(实时数据)相结合，将简单的数据字段与场景规则语句相结合，将流动的事件与可复用、组合应用的场景规则相结合，提高了安全预警的分析处理力度，提高了预警事件生成的自适应性。

[0057] 本发明包含范式化引擎、数据流语义分析引擎、安全分析模型计算引擎三大类引擎，每一类引擎按照不同的复杂事件，通过不同的规则模块定义配置，处理数据日志，在实现对数据流按照场景建模语义分析的基础上，基于事件窗即时间窗或者日志长度窗口方式，对事件建立场景模型，从而生成预警事件。该方法中的范式化引擎将日志数据进行特定处理，形成相同(固定字段集合+x)的格式，其中的x表示备用字段，固定字段集合用于分析生成实时预警事件，这些固定字段集合是依据经验形成的，对产品所属厂商的依赖度小。数据流语义分析引擎对从不同方面获取的、连续的、流动的信息进行预警建模语义分析，提取实例，为生成预警作准备。安全分析模型计算引擎建立威胁模型，基于自定义的事件窗口，提取出正在发生事件的关联性，以此生成预警，揭示将要发生的事件。场景建模是安全事件驱动的，区别于以往的纯数据驱动。

[0058] 该发明遵循标准CEP的主要流程，并加以提炼，形成了一套基于安全事件场景的实时预警方法，其主要步骤包括：1.数据预处理、范式化；2.数据语义分析，为预警生成做准备；3.复杂事件场景建模与数据关联分析。每个主要步骤下包含多个从步骤用以辅助各主要功能引擎。

[0059] 本发明的技术方案是：

[0060] 基于复杂事件处理的实时安全预警方法，具体包括以下步骤：

[0061] (1)利用范式化引擎将采集到的安全数据进行日志字段分割，并依据字段的不同规范化要求对字段进行规范化，按照期望输出的字段，关联知识库信息，加强产生符合分析格式的日志字段；

[0062] (2)利用数据流语义分析引擎，依据将要作为场景建模的复杂事件实例，进行数据上下文分析，依据标准化的分析字段模板，分析映射流数据，作为下一步骤的关键元信息；

[0063] (3)利用安全分析模型计算引擎，在分析规则计算模块中，基于点事件、边缘事件、间隔事件这三类不同的基于时间的事件，进行按场景分析，生成预警事件。其中的点事件、边缘事件、间隔事件在以下每个步骤的详细运行过程中再进行阐述。

[0064] 步骤(1)中，范式化引擎的运行过程为：

[0065] 采集程序将采集到的日志数据依次发送到Kafka，Kafka中的数据依次进入Storm的过滤器引擎，依据不同日志类别，按照处理的最细粒度进一步分为日志类型匹配、日志数据字段匹配、字段合并去重、与资产数据等离线知识库数据相关联，进行关联信息处理及关联字段处理，将不同日志加强分析后的字段加入到对应日志的字段集合中形成最终范式化结果。其中：

[0066] 1)Storm从Kafka服务器上对应topic中获取数据(预置Kafka的topic和Storm的topology的之间的映射关系)，同一类日志配置一个topic，其中同一类日志可能是不同厂商按其自己的格式规范发送过来的格式不同的日志；去重、去噪模块将数据组织成{LogID,Name,Reg,Seperator,DataModelID}的形式，其中LogID是每类日志的一个唯一标识号，Name是日志名，Reg是日志正则表达式用于区分各类不同日志进入不同操作流程，Seperator是用于拆分日志中字段的分隔符，DataModelID是依据日志数据的大类、细类以及具体作用拼合的用于标识不同厂商但类型相同的日志的数据模型号，该字段主要作用是：日志合并，去重、去噪。

[0067] 2)经过去重、去噪后的日志再次被传送到Kafka的预置topic中(不同于过滤器取数的topic)，Storm从topic取数据，与资产数据等离线知识库数据相关联，进行关联信息处理及关联字段处理，这个步骤称为加强。

[0068] 3)由数据格式化模块将不同日志加强分析后的字段加入到对应日志的字段集合中形成最终范式化结果。

[0069] 其具体步骤为：

[0070] 1)字段正则匹配、拆分、去重、去噪

[0071] 使用正则表达式加特殊标识的方法对日志数据类型进行匹配识别，为了将特定的字段处理成统一字段格式，将各类日志已拆分的字段依据规范化标准进行处理，如日志生成时间，对发送过来有数字有英文表示法的数据处理后合并，最终统一标准化成标准时间戳格式。将不同厂商的同类型日志进行合并，并使用md5值判定的方法进行日志的去重，即将数据各字段联合计算md5值，如值相同即为重复。将日志中的字段名以规范好的字段约束，以便后续数据加强处理。

[0072] 2)由知识库及已知日志字段推导未知字段

[0073] 使用类SQL语句联系已有知识库数据，进行关联分析，按序分步推导出相关字段，需要关联分析推导出的字段主要有：源或目的地址的位置信息、资产信息(包括所属应用系统、所属网络、硬件设备信息)。每种类型标准化后的字段加上加强后需要的字段新增字段形成范式化后最终字段集合，需要发送到数据检索引擎的字段置为输出项，其他备用字段置为非输出项。

[0074] 3)联合推导形成范式化最终字段

[0075] 依据加强器模块记录的类SQL及日志字段之间的关联，将不同日志加强分析后的字段加入到对应日志的字段集合中，从而达到字段处理的目的，最终完成数据范式化。

[0076] 步骤(2)中，数据流语义分析引擎的运行过程为：

[0077] 将上一步骤中经过范式化的流数据从Kafka中对应的topic取出，将这些数据进行上下文语义分析，并且按照对应的标准化复杂事件字段模板进行映射，经过语义分析的实

时数据才能进入Esper的事件窗，作为复杂事件。

[0078] 数据流语义分析引擎运行的具体步骤为：

[0079] 1)复杂事件字段标准化

[0080] 复杂事件字段标准化模块中，存储着范式化后日志数据的模型号、类型、字段名称等重要信息，这些信息每一行数据是一个规则元组，是后续复杂事件提取的规则。该模板可以随着日志种类的增加而增加，以提供更完善的语义分析能力。

[0081] 2)复杂事件字段提取

[0082] 复杂事件由连续的、流动的数据组成，这些数据在复杂事件实例映射模块中，依据标准复杂事件字段模块的规则，映射成一条条实例。

[0083] 步骤(3)中，安全分析模型计算引擎的运行过程为：

[0084] 通过步骤(2)得到的经过语义分析的标准字段，进入该步骤中建立的模型引擎中，分析，关联，最终生成预警。

[0085] 复杂事件场景建模引擎的具体步骤为：

[0086] 1)场景建模，生成预警事件

[0087] 分析规则计算模块是复杂事件分析引擎中最重要的模块。该模块将经过复杂事件字段提取模块提取的复杂事件，通过Esper技术使用EPL语法进行关联场景分析。该模块还包括场景建模规则表，这些表是通过预置或者人工生成的方式定义的。两种定义如下。

[0088] a)预置

[0089] 针对各类日志最基本的安全事件场景，以事件为单位，安全事件是指可能对系统或者系统中某个模块产生威胁的事件，这些事件里的阀值是可以配置的，配置之后重启预警事件生成引擎即可生效。

[0090] b)人工生成

[0091] 从用户角度而言，用户认为的某一类(或某几类)数值可能对系统造成威胁的安全事件，人工生成的场景就保证了安全预警框架的灵活性，做到临界值可配置。

[0092] 在场景建模中，复杂事件的场景中的事件主要有三类，即：点事件、边缘事件、间隔事件。三类事件定义如下。

[0093] a)点事件

[0094] 在某一时刻或者基于某一条复杂事件进行分析推导出的预警事件，这类事件类似于传统预警事件中的基于阈值推断的事件，指的是某一瞬间发生的事件，也是最为简单的一种。该事件经过场景建模规则表，依据规则表里某字段的阈值，生成预警。

[0095] b)边缘事件

[0096] 只对某一同类型事件进行的分析推导出的预警事件，但是这类事件是在最近的一个连续时间段的事件，或者最近的连续条数的事件，这里的连续事件条数也是可配置的。通过场景建模规则表，依据规则表里的规则，生成预警。

[0097] c)间隔事件

[0098] 对复杂事件中的某几类事件的分析推导出的预警事件，间隔事件是复杂事件中组合最多的一种情况，不局限于一类日志，对流数据通过场景建模规则表里的规则，进行分析，生成预警。

[0099] 需指出，上述的三种场景事件模型在复杂事件分析引擎中是并行的、没有先后主

次关系。这也使复杂事件分析引擎对连续的复杂事件生成预警更具多样性，而不局限于某一种单一的预警生成。

[0100] 生成的预警以用户可接受的方式展现在前台，以供相关人员发现系统可能存在的威胁。

[0101] 2)标准化预警格式建立

[0102] 这里的标准化预警格式建立是由标准化预警输出模板进行预先建立的，即是安全分析人员最关心的预警生成的关键格式，这里的格式是预置好的，所有的预警输出都是一致的，主要包括预警事件的名称、预警产生的原因字段，预警产生时间(实际为依据日志定位到的操作行为事件)等关键数据。

[0103] 以上显示和描述了本发明的基本原理和主要特征和本发明的优点。本行业的技术人员应该了解，本发明不受上述实施例的限制，上述实施例和说明书中描述的只是说明本发明的原理，在不脱离本发明精神和范围的前提下，本发明还会有各种变化和改进，这些变化和改进都落入要求保护的本发明范围内。本发明要求保护范围由所附的权利要求书及其等效物界定。

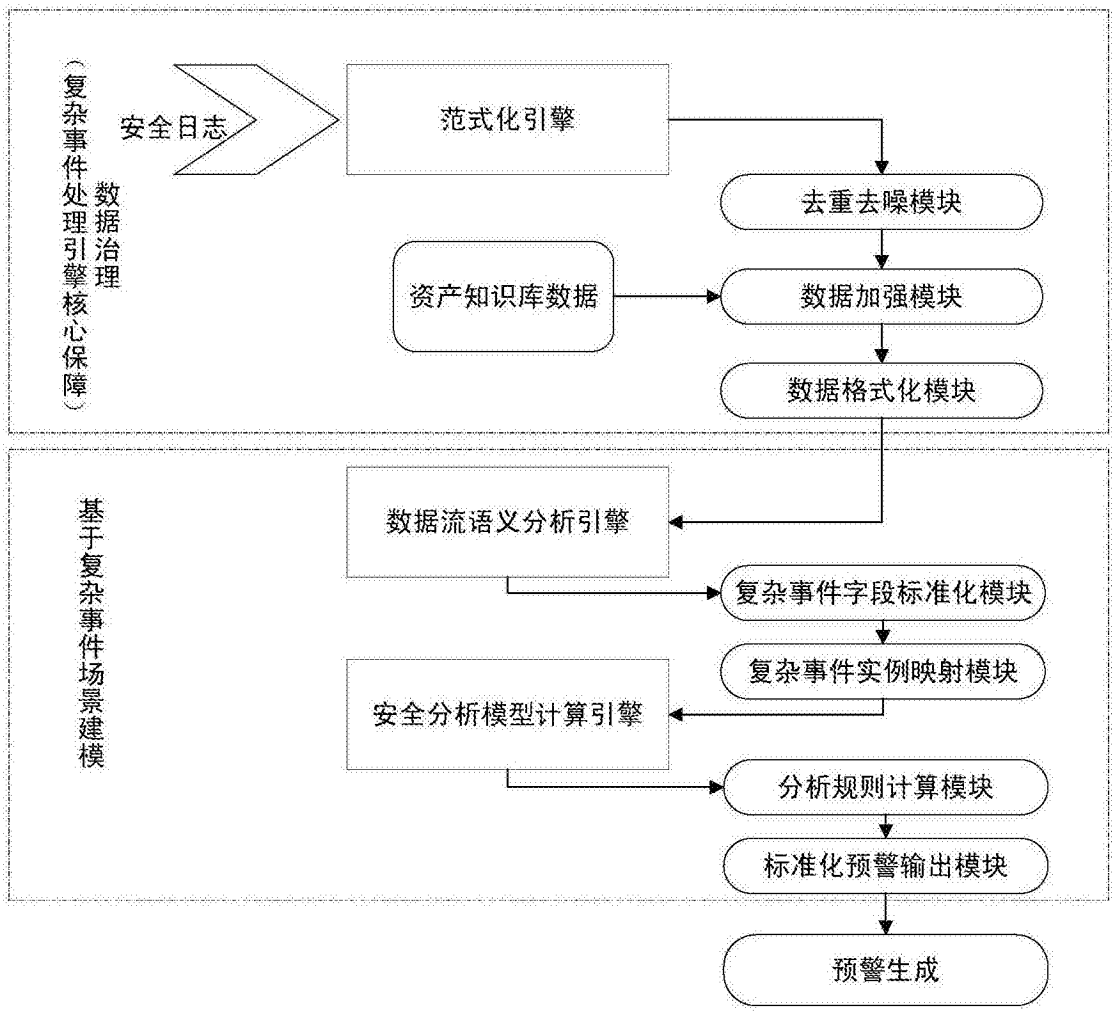

（复杂事件处理引擎核心保障）数据治理
安全日志
范式化引擎
去重去噪模块
资产知识库数据
数据加强模块
数据格式化模块
基于复杂事件场景建模
数据流语义分析引擎
复杂事件字段标准化模块
复杂事件实例映射模块
安全分析模型计算引擎
分析规则计算模块
标准化预警输出模块
预警生成

图1

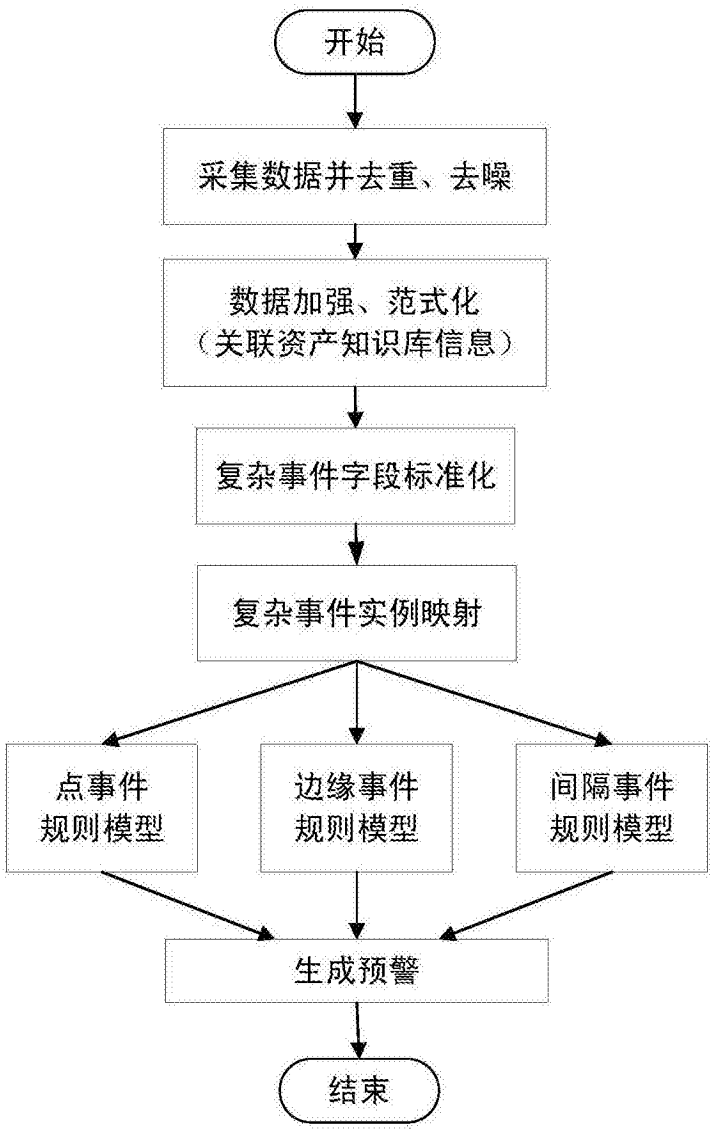

开始
采集数据并去重、去噪
数据加强、范式化
（关联资产知识库信息）
复杂事件字段标准化
复杂事件实例映射
点事件
规则模型
边缘事件
规则模型
间隔事件
规则模型
生成预警
结束

图2

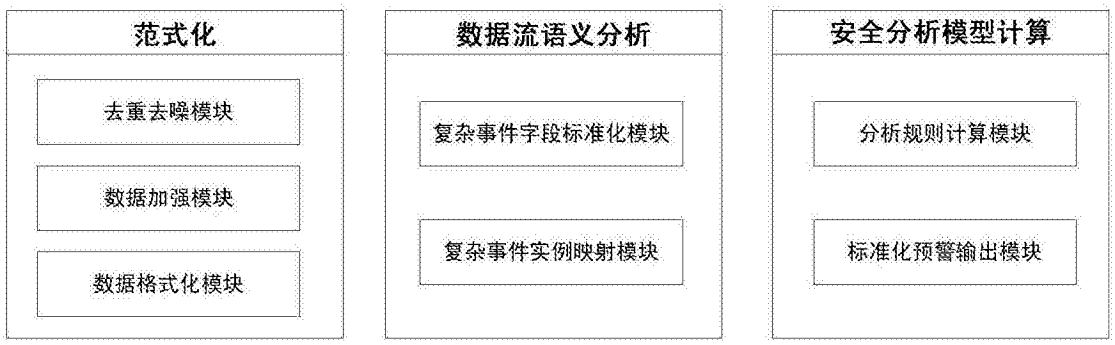

范式化
去重去噪模块
数据加强模块
数据格式化模块
数据流语义分析
复杂事件字段标准化模块
复杂事件实例映射模块
安全分析模型计算
分析规则计算模块
标准化预警输出模块

图3