(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113343228 B
(45)授权公告日 2023.11.10

(21)申请号 202110737078.1
(22)申请日 2021.06.30
(65)同一申请的已公布的文献号
申请公布号 CN 113343228 A
(43)申请公布日 2021.09.03
(73)专利权人 北京天融信网络安全技术有限公司
地址 100000 北京市海淀区上地东路1号院3号楼四层
专利权人 北京天融信科技有限公司
北京天融信软件有限公司
(72)发明人 姚善 杨圣峰
(74)专利代理机构 北京超凡宏宇知识产权代理有限公司 11463
专利代理师 唐正瑜
(51)Int.Cl.
*G06F 21/55*(2013.01)
*G06F 21/57*(2013.01)
*G06N 3/0464*(2023.01)
*G06N 3/08*(2023.01)
*G06F 18/24*(2023.01)
*G06F 18/22*(2023.01)

(56)对比文件
CN 111611495 A,2020.09.01
CN 103281341 A,2013.09.04
CN 112333196 A,2021.02.05
CN 112422484 A,2021.02.26
CN 101521672 A,2009.09.02
CN 101668012 A,2010.03.10
CN 103996077 A,2014.08.20
CN 108737147 A,2018.11.02
CN 109255237 A,2019.01.22
CN 109358602 A,2019.02.19
CN 111654489 A,2020.09.11
CN 112235312 A,2021.01.15
CN 112351004 A,2021.02.09
CN 112637194 A,2021.04.09
CN 112738115 A,2021.04.30
US 2017093902 A1,2017.03.30
US 2020177469 A1,2020.06.04
US 2021176264 A1,2021.06.10
US 8407798 B1,2013.03.26 (续)

审查员 马秋佳

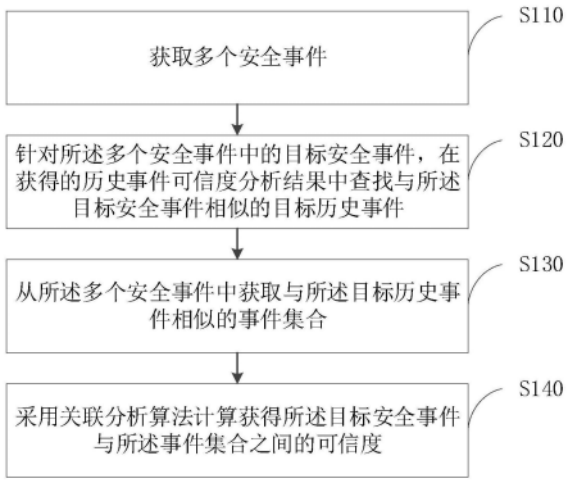
权利要求书2页 说明书10页 附图2页

(54)发明名称

事件可信度分析方法、装置、电子设备及可读存储介质

(57)摘要

本申请提供一种事件可信度分析方法、装置、电子设备及可读存储介质，涉及网络安全技术领域。该方法在对目标安全事件进行分析时，从历史事件可信度分析结果中查找与其相似的目标历史事件，然后获取与目标历史事件相似的事件结合，并利用关联分析算法计算获得目标安全事件与事件集合之间的可信度，以获得目标安全事件的可信度，无需通过人工识别，效率更高。并且，通过结合历史事件可信度分析结果，对安全事件的可信度分析提供一定程度上的数据支撑，使得分析结果更准确。




CN 113343228 B

[转续页]

[接上页]

(56)对比文件

蔡红云.基于信任领域和评价可信度量的信任模型研究.计算机研究与发展.2011,全文.

李远远.无线闭塞中心安全风险评估研究.中国优秀硕士学位论文数据库 工程科技II辑.2017,全文.

唐湘滟;程杰仁;刘博艺;郑兆华;周静荷.基于Apriori算法的安全事件二级关联方法.网络安全技术与应用.2017,(第01期),全文.

邱荣斌;许榕生.一种网络安全信息的综合关联分析方法.福建电脑.2006,(第02期),全文.

刘育楠;徐震;王若琦.一种基于计划识别的安全事件关联分析方法.信息工程大学学报.2015,(第01期),全文.

1.一种事件可信度分析方法,其特征在于,所述方法包括:

获取多个安全事件,其中,安全事件是指安全系统检测到威胁网络安全的任何一个行为所产生的事件;

针对所述多个安全事件中的目标安全事件,在获得的历史事件可信度分析结果中查找与所述目标安全事件相似的目标历史事件,其中,所述目标安全事件是指所述多个安全事件中的任意一个安全事件,所述历史事件可信度分析结果包括历史事件与可信度分析结果的对应关系,历史事件是指历史的安全事件;

从所述多个安全事件中获取与所述目标历史事件相似的事件集合,所述事件集合包含至少一个安全事件,其中,所述事件集合中的安全事件与所述目标历史事件的类别相同,和/或与所述目标历史事件发生的时间相近;

采用关联分析算法计算获得所述目标安全事件与所述事件集合之间的可信度。

2.根据权利要求1所述的方法,其特征在于,所述从所述多个安全事件中获取与所述目标历史事件相似的事件集合,包括:

对所述多个安全事件进行分类,获得每个安全事件对应的类别;

对所述多个安全事件按照时间顺序进行排序,获得事件序列;

根据每个安全事件对应的类别以及所述事件序列获取与所述目标历史事件相似的事件集合。

3.根据权利要求2所述的方法,其特征在于,所述对所述多个安全事件进行分类,获得每个安全事件对应的类别,包括:

按照以下至少一个分类维度对所述多个安全事件进行分类,获得每个安全事件对应的类别,所述至少一个分类维度包括:来源、目的、协议类型、端口、事件性质。

4.根据权利要求1所述的方法,其特征在于,所述采用关联分析算法计算获得所述目标安全事件与所述事件集合之间的可信度,包括:

采用Apriori算法计算获得所述目标安全事件的第一支持度以及所述目标安全事件与所述事件集合的第二支持度;

根据所述第一支持度以及所述第二支持度计算获得所述目标安全事件与所述事件集合之间的可信度。

5.根据权利要求1所述的方法,其特征在于,所述采用关联分析算法计算获得所述目标安全事件与所述事件集合之间的可信度之后,还包括:

根据所述可信度获取对所述目标安全事件的可信度分析结果;

将所述目标安全事件标注对应的可信度分析结果,并存入所述历史事件可信度分析结果中。

6.根据权利要求1所述的方法,其特征在于,所述获取多个安全事件,包括:

获取原始事件,其中,所述原始事件是指网络设备和/或WEB类应用上的所有网络行为所产生的事件;

采用神经网络模型对所述原始事件进行异常检测,获得多个安全事件。

7.根据权利要求1所述的方法,其特征在于,所述获取多个安全事件,包括:

获取多个初始安全事件;

对所述多个初始安全事件进行标准化形式处理,获得处理后的多个初始安全事件;

按照预设的过滤规则对所述处理后的多个初始安全事件进行过滤，获得多个安全事件。

8.一种事件可信度分析装置，其特征在于，所述装置包括：

事件获取模块，用于获取多个安全事件，其中，安全事件是指安全系统检测到威胁网络安全的任何一个行为所产生的事件；

历史事件查找模块，用于针对所述多个安全事件中的目标安全事件，在获得的历史事件可信度分析结果中查找与所述目标安全事件相似的目标历史事件，其中，所述目标安全事件是指所述多个安全事件中的任意一个安全事件，所述历史事件可信度分析结果包括历史事件与可信度分析结果的对应关系，历史事件是指历史的安全事件；

事件集合获取模块，用于从所述多个安全事件中获取与所述目标历史事件相似的事件集合，所述事件集合包含至少一个安全事件，其中，所述事件集合中的安全事件与所述目标历史事件的类别相同，和/或与所述目标历史事件发生的时间相近；

可信度计算模块，用于采用关联分析算法计算获得所述目标安全事件与所述事件集合之间的可信度。

9.一种电子设备，其特征在于，包括处理器以及存储器，所述存储器存储有计算机可读取指令，当所述计算机可读取指令由所述处理器执行时，运行如权利要求1-7任一所述的方法。

10.一种可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时运行如权利要求1-7任一所述的方法。

# 事件可信度分析方法、装置、电子设备及可读存储介质

## 技术领域

[0001] 本申请涉及网络安全技术领域，具体而言，涉及一种事件可信度分析方法、装置、电子设备及可读存储介质。

## 背景技术

[0002] 随着计算机技术和网络技术的发展，网络安全问题也越来越受到重视。为了保证网络系统的安全，通常需要对威胁网络安全的任何一个行为进行报警，即产生安全事件。安全事件由安全系统生成，如防火墙、漏洞扫描系统、防病毒系统等，这些安全系统都会产生大量的安全事件。而安全系统通常是通过简单的规则匹配来识别这些攻击行为，进而产生安全事件，所以，安全系统产生的安全事件可能存在一些误报，可信度并不高，而安全管理员仅仅通过人为经验来识别这些安全事件的可信度，效率低下且准确度不高，使得安全管理工作变得越来越困难。

## 发明内容

[0003] 本申请实施例的目的在于提供一种事件可信度分析方法、装置、电子设备及可读存储介质，用以改善现有技术中通过人工识别安全事件的可信度的方式导致的效率低下且准确度不高的问题。

[0004] 第一方面，本申请实施例提供了一种件可信度分析方法，所述方法包括：获取多个安全事件；针对所述多个安全事件中的目标安全事件，在获得的历史事件可信度分析结果中查找与所述目标安全事件相似的目标历史事件；从所述多个安全事件中获取与所述目标历史事件相似的事件集合，所述事件集合包含至少一个安全事件；采用关联分析算法计算获得所述目标安全事件与所述事件集合之间的可信度。

[0005] 在上述实现过程中，在对目标安全事件进行分析时，可以从历史事件可信度分析结果中查找与其相似的目标历史事件，然后获取与目标历史事件相似的事件结合，并利用关联分析算法计算获得目标安全事件与事件集合之间的可信度，以获得目标安全事件的可信度，无需通过人工识别，效率更高。并且，通过结合历史事件可信度分析结果，对安全事件的可信度分析提供一定程度上的数据支撑，使得分析结果更准确。

[0006] 可选地，所述从所述多个安全事件中获取与所述目标历史事件相似的事件集合，包括：

[0007] 对所述多个安全事件进行分类，获得每个安全事件对应的类别；

[0008] 对所述多个安全事件按照时间顺序进行排序，获得事件序列；

[0009] 根据每个安全事件对应的类别以及所述事件序列获取与所述目标历史事件相似的事件集合，其中，所述事件集合中的安全事件与所述目标历史事件的类别相同，和/或与所述目标历史事件发生的时间相近。

[0010] 在上述实现过程中，通过根据安全事件对应的类别以及事件序列来获取与目标历史事件相似的安全事件，从而可以找到一些相似的安全事件来对目标安全事件的可信度进

行支撑，进而获得更准确的可信度。

[0011] 可选地，所述对所述多个安全事件进行分类，获得每个安全事件对应的类别，包括：

[0012] 按照以下至少一个分类维度对所述多个安全事件进行分类，获得每个安全事件对应的类别，所述至少一个分类维度包括：来源、目的、协议类型、端口、事件性质。这样可以有效根据安全事件的类别查找到相似的安全事件。

[0013] 可选地，所述采用关联分析算法计算获得所述目标安全事件与所述事件集合之间的可信度，包括：

[0014] 采用Apriori算法计算获得所述目标安全事件的第一支持度以及所述目标安全事件与所述事件集合的第二支持度；

[0015] 根据所述第一支持度以及所述第二支持度计算获得所述目标安全事件与所述事件集合之间的可信度。

[0016] 在上述实现过程中，通过Apriori算法来计算可信度，从而可以通过分析与目标安全事件和事件集合之间的关联性来获得更准确的可信度。

[0017] 可选地，所述采用关联分析算法计算获得所述目标安全事件与所述事件集合之间的可信度之后，还包括：

[0018] 根据所述可信度获取对所述目标安全事件的可信度分析结果；

[0019] 将所述目标安全事件标注对应的可信度分析结果，并存入所述历史事件可信度分析结果中。这样可以为后续的安全事件的可信度分析提供更多的数据支撑。

[0020] 可选地，所述获取多个安全事件，包括：

[0021] 获取原始事件；

[0022] 采用神经网络模型对所述原始事件进行异常检测，获得多个安全事件。这样可以更准确地检测出威胁网络安全的安全事件。

[0023] 可选地，所述获取多个安全事件，包括：

[0024] 获取多个初始安全事件；

[0025] 对所述多个初始安全事件进行标准化形式处理，获得处理后的多个初始安全事件；

[0026] 按照预设的过滤规则对所述处理后的多个初始安全事件进行过滤，获得多个安全事件。

[0027] 在上述实现过程中，通过对初始安全事件进行标准化形式处理和过滤处理，从而可以筛选出一些不符合规范和要求的安全事件，以提高后续对安全事件进行可信度分析的效率。

[0028] 第二方面，本申请实施例提供了一种事件可信度分析装置，所述装置包括：

[0029] 事件获取模块，用于获取多个安全事件；

[0030] 历史事件查找模块，用于针对所述多个安全事件中的目标安全事件，在获得的历史事件可信度分析结果中查找与所述目标安全事件相似的目标历史事件；

[0031] 事件集合获取模块，用于从所述多个安全事件中获取与所述目标历史事件相似的事件集合，所述事件集合包含至少一个安全事件；

[0032] 可信度计算模块，用于采用关联分析算法计算获得所述目标安全事件与所述事件

集合之间的可信度。

[0033] 可选地，所述事件集合获取模块，用于对所述多个安全事件进行分类，获得每个安全事件对应的类别；对所述多个安全事件按照时间顺序进行排序，获得事件序列；根据每个安全事件对应的类别以及所述事件序列获取与所述目标历史事件相似的事件集合，其中，所述事件集合中的安全事件与所述目标历史事件的类别相同，和/或与所述目标历史事件发生的时间相近。

[0034] 可选地，所述事件集合获取模块，用于按照以下至少一个分类维度对所述多个安全事件进行分类，获得每个安全事件对应的类别，所述至少一个分类维度包括：来源、目的、协议类型、端口、事件性质。

[0035] 可选地，所述可信度计算模块，用于采用Apriori算法计算获得所述目标安全事件的第一支持度以及所述目标安全事件与所述事件集合的第二支持度；根据所述第一支持度以及所述第二支持度计算获得所述目标安全事件与所述事件集合之间的可信度。

[0036] 可选地，所述装置还包括：

[0037] 存储模块，用于根据所述可信度获取对所述目标安全事件的可信度分析结果；将所述目标安全事件标注对应的可信度分析结果，并存入所述历史事件可信度分析结果中。

[0038] 可选地，所述事件获取模块，用于获取原始事件；采用神经网络模型对所述原始事件进行异常检测，获得多个安全事件。

[0039] 可选地，所述事件获取模块，用于获取多个初始安全事件；对所述多个初始安全事件进行标准化形式处理，获得处理后的多个初始安全事件；按照预设的过滤规则对所述处理后的多个初始安全事件进行过滤，获得多个安全事件。

[0040] 第三方面，本申请实施例提供一种电子设备，包括处理器以及存储器，所述存储器存储有计算机可读取指令，当所述计算机可读取指令由所述处理器执行时，运行如上述第一方面提供的所述方法中的步骤。

[0041] 第四方面，本申请实施例提供一种可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时运行如上述第一方面提供的所述方法中的步骤。

[0042] 本申请的其他特征和优点将在随后的说明书阐述，并且，部分地从说明书中变得显而易见，或者通过实施本申请实施例了解。本申请的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

## 附图说明

[0043] 为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本申请的某些实施例，因此不应被看作是对范围的限定，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他相关的附图。

[0044] 图1为本申请实施例提供的一种用于执行事件可信度分析方法的电子设备的结构示意图；

[0045] 图2为本申请实施例提供的一种事件可信度分析方法的流程图；

[0046] 图3为本申请实施例提供的一种事件可信度分析装置的结构框图。

## 具体实施方式

[0047] 下面将结合本申请实施例中附图，对本申请实施例中的技术方案进行清楚、完整地描述。

[0048] 本申请实施例提供一种事件可信度分析方法，该方法对目标安全事件进行分析时，可以从历史事件可信度分析结果中查找与其相似的目标历史事件，然后获取与目标历史事件相似的事件结合，并利用关联分析算法计算获得目标安全事件与事件集合之间的可信度，以获得目标安全事件的可信度，无需通过人工识别，效率更高。并且，通过结合历史事件可信度分析结果，对安全事件的可信度分析提供一定程度上的数据支撑，使得分析结果更准确。

[0049] 请参照图1，图1为本申请实施例提供的一种用于执行事件可信度分析方法的电子设备的结构示意图，所述电子设备可以包括：至少一个处理器110，例如CPU，至少一个通信接口120，至少一个存储器130和至少一个通信总线140。其中，通信总线140用于实现这些组件直接的连接通信。其中，本申请实施例中设备的通信接口120用于与其他节点设备进行信令或数据的通信。存储器130可以是高速RAM存储器，也可以是非易失性的存储器(non-volatile memory)，例如至少一个磁盘存储器。存储器130可选的还可以是至少一个位于远离前述处理器的存储装置。存储器130中存储有计算机可读取指令，当所述计算机可读取指令由所述处理器110执行时，电子设备执行下述图2所示方法过程。

[0050] 可以理解，图1所示的结构仅为示意，所述电子设备还可包括比图1中所示更多或者更少的组件，或者具有与图1所示不同的配置。图1中所示的各组件可以采用硬件、软件或其组合实现。

[0051] 请参照图2，图2为本申请实施例提供的一种事件可信度分析方法的流程图，该方法包括如下步骤：

[0052] 步骤S110：获取多个安全事件。

[0053] 其中，安全事件是指安全系统检测到威胁网络安全的任何一个行为所产生的事件，安全事件也可以理解为是威胁网络安全的行为，即该行为可以理解为一个安全事件。这些安全事件可以是安全系统对来自于网络设备和/或WEB类应用的事件进行检测获得的，包括如网络设备被攻击而产生的安全事件，或者如Web漏洞、Web恶意文件、恶意代码等安全事件，或者是通过防火墙、IDS、杀毒软件、系统日志等采集的报警事件。安全系统可以网络设备和/或WEB类应用进行扫描，以扫描其网络设备和/或WEB类应用上所产生的行为(即事件)，然后采用一些规则来检测这些行为是否是威胁网络安全的行为，从而获得安全事件。

[0054] 可以理解地，各个网络设备可以在产生安全事件后，按照本申请实施例提供的可信度分析方法对安全事件进行可信度分析后，再将安全事件发送给后端设备，这样后端设备的安全管理员可以直接根据安全事件的可信度对安全事件进行处理，这种情况下，上述的电子设备即为网络设备。或者各个网络设备也可以是将产生的安全事件发送给后端设备，即电子设备，此时电子设备后获得各个网络设备传输过来的安全事件，然后统一对这些安全事件进行可信度分析，并且由于获得的是各个网络设备的安全事件，所以可以对这些安全事件进行整合，从而可以通过关联分析算法挖掘出更多安全事件之间的关联关系，以对安全事件进行更准确地可信度分析。

[0055] 步骤S120：针对所述多个安全事件中的目标安全事件，在获得的历史事件可信度

分析结果中查找与所述目标安全事件相似的目标历史事件。

[0056] 历史事件可信度分析结果是指对历史的安全事件进行可信度分析后获得的结果，其存储有各个历史事件对应的可信度分析结果，可信度分析结果包括可信和不可信，对于历史事件的可信度分析方法也是采用本申请提供的分析方法获得并经过人工确认了的，准确度较高。

[0057] 需要说明的是，在上述电子设备为各个网络设备时，各个网络设备中均各自存储有对应的历史事件可信度分析结果，其各自的历史事件可信度分析结果是网络设备对历史的安全事件进行可信度分析获得的。若电子设备为后端设备时，则电子设备中存储有一份历史事件可信度分析结果，其是对所有历史的安全事件进行可信度分析获得的，信息量更多，所以在后续进行可信度分析时，可以提供更多的数据支撑，准确度更高。

[0058] 其中，目标安全事件可以是指多个安全事件中的任意一个安全事件，针对每个安全事件的可信度分析方法均是相同的，为了描述的便利，本申请中以其中一个安全事件称为目标安全事件为例进行说明。

[0059] 在对目标安全事件进行可信度分析时，可以从历史事件可信度分析结果中查找与目标安全事件相似的目标历史事件。例如，可以提取目标安全事件的流量特征，包括源地址、目的地址、协议类型、事件性质(如是攻击行为的事件或Web漏洞事件等)、事件中所包含的各个字段特征等，历史事件可信度分析结果中存储的可以是历史事件的流量特征与可信度分析结果的对应关系，这样可以通过将目标安全事件的流量特征与各个历史事件的流量特征进行相似度匹配，然后将流量特征相同的数量最多的历史事件作为与目标安全事件最相似的目标历史事件。

[0060] 可以理解的，获得的目标历史事件的数量不止一个，也可以有多个，如可以将相似度大于设定相似度的历史事件均作为目标历史事件。

[0061] 步骤S130:从所述多个安全事件中获取与所述目标历史事件相似的事件集合。

[0062] 其中，事件集合包含至少一个安全事件。由于历史事件可信度分析结果中包括有各个历史事件对应的可信度分析结果，这些可信度分析结果能够在一定程度上影响当前的安全事件的可信度，所以通过获取与目标历史事件相似的事件集合来对目标安全事件进行可信度分析能够更准确。

[0063] 其中，获取与目标历史事件相似的事件集合的方式也可以与上述获得与目标安全事件相似的目标历史事件的方式类似，如也可以从多个安全事件中获取与目标历史事件的流量特征相似的安全事件，即将目标历史事件的流量特征与各个安全事件的流量特征进行相似度计算，将相似度大于设定相似度的安全事件作为与目标历史事件相似的安全事件，加入到事件集合中。其中，在相似度计算时，可以将目标历史事件的流量特征和各个安全事件的流量特征分别按照设定的规则映射为一特征向量，然后计算目标历史事件的特征向量与各个安全事件的特征向量之间的余弦距离，如果余弦距离大于预设值，则认为两个事件的相似度大于设定相似度，则可以将相似度大于设定相似度的这些安全事件作为与目标历史事件相似的安全事件，这些安全事件即作为事件集合。

[0064] 步骤S140:采用关联分析算法计算获得所述目标安全事件与所述事件集合之间的可信度。

[0065] 关联分析算法是指用于挖掘数据之间的关联关系的算法，其可以有Apriori算法、

FP-Tree算法、Eclat算法以及灰色关联法等。

[0066] 其中，在关联分析算法中，其可信度的计算公式如下：

[0067] $$confidence(A \Rightarrow B) = P(B|A) = \frac{\sup\ port(A \cup B)}{\sup\ port(A)}$$；

[0068] 其中，A表示目标安全事件，B表示事件集合，$confidence(A \Rightarrow B)$表示A的可信度，support(A∪B)表示A和B的支持度，即表示A和B同时出现在事务集合中的次数，support(A)表示A的支持度，即表示A出现在事务集合中的次数。

[0069] 在一些实施方式中，可以采用Apriori算法计算获得目标安全事件的第一支持度以及目标安全事件与事件集合的第二支持度，然后根据第一支持度以及第二支持度计算获得目标安全事件与事件集合之间的可信度。

[0070] 可以理解地，多个安全事件的数量可以是很多的，如有80个安全事件，在进行关联分析时，可以将在各个时间点所获得的安全事件作为一条事务，如在T1时刻，获得有5条安全事件，在T2时刻，获得有4条安全事件，一共有10个时刻的事件，则对应有10条事务。然后将这些时刻对应的安全事件组成事务集合，即事务集合可包括上述的10条事务，或者事务集合中还可以包含历史时段获取到的安全事件，这样可以利用更多的信息来挖掘出更多的关联关系。一条事务可以理解为是事务集合中的一个项集，即上述示例的事务集合包括有10条事务，每个事务又可以包括多个安全事件，每个安全事件可称为项，如T1时刻对应的事务包含有5个项。

[0071] 在计算支持度时，比如目标安全事件为事件A，事件集合包括事件B、C、D，则在计算事件A的支持度时，可以先统计事件A在各个事务中出现的次数，如事件A出现在5个事务中，则事件A的支持度则为5(即上述的第一支持度)，同理，对于事件A和事件集合的支持度是指统计事件A、B、C、D在各个事务中出现的次数，如有两个事务中出现了这四个事件，则事件A和事件集合的支持度即为2(即上述的第二支持度)。然后按照上述可信度的计算公式，即可计算获得事件A的可信度为2/5。

[0072] 由于上述获得的事件B、C、D是与目标历史事件相似的事件，而目标历史事件是已经进行了可信度分析的事件，所以目标历史事件的可信度分析结果在一定程度上能够对事件A的可信度产生影响，进而通过关联分析算法分析与事件A关联的事件B、C、D，这样可以结合历史分析结果以及事件B、C、D对事件A的可信度进行支撑，从而获得更准确的可信度。

[0073] 同理，针对多个安全事件中的其他安全事件，也可以按照上述同样的方式获得各个安全事件的可信度。

[0074] 另外，为了便于对事件进行关联分析，还可以预先基于统计规律以及贝叶斯条件概率理论的基础对每类安全事件、事件序列、历史事件可信度分析结果进行抽象，得到一种数值化的度量描述，然后在进行可信度分析时，可以直接基于数值化的度量描述进行后续的计算过程，效率更高。

[0075] 在获得各个安全事件的可信度后，可以按照可信度大小对各个安全事件进行排序，可信度越大说明安全事件越可信，即危险性越小，可信度越小说明安全事件越不可信，即危险性越大。可以按照可信度由小到大排序后，可以将排序后的安全事件输出，这样安全管理员可以按照排序优先对可信度小的安全事件进行安全性排查，从而可以按照事件的危

险程度来进行处理，以及时处理危险性大的事件，确保网络安全。

[0076] 在一些实施方式中，还可以基于可信度判断各个安全事件是否可信，如可信度大于设定值，则认为对应的安全事件可信，反之则不可信。例如，若上述示例中的事件A的可信度大于设定值，则认为事件A是可信的，而事件A的可信度大于设定值则表明事件A与事件B、C、D之间具有强关联性，若事件A是可信的，则可以确定事件B、C、D也是可信的，反之，若事件A是不可信的，则确定事件B、C、D也是不可信的。所以，若是为了判断各个安全事件是否是可信时，则可以无需再计算获得事件B、C、D各自的可信度了，即不需要重复计算，而是可以直接根据事件A是否可信来判断事件B、C、D是否可信，从而可提高对安全事件的可信分析的效率。

[0077] 在上述实现过程中，在对目标安全事件进行分析时，可以从历史事件可信度分析结果中查找与其相似的目标历史事件，然后获取与目标历史事件相似的事件结合，并利用关联分析算法计算获得目标安全事件与事件集合之间的可信度，以获得目标安全事件的可信度，无需通过人工识别，效率更高。并且，通过结合历史事件可信度分析结果，对安全事件的可信度分析提供一定程度上的数据支撑，使得分析结果更准确。

[0078] 在上述实施例的基础上，上述获取多个安全事件的方式中，还可以先获取原始事件，然后采用神经网络模型对原始事件进行异常检测，获得多个安全事件。

[0079] 其中，原始事件可以是指网络设备和/或WEB类应用上的所有网络行为，电子设备可以对这些网络行为进行异常检测，如检测这些网络行为是否是威胁网络安全的行为，即是否是安全事件。具体检测的方式可以是通过神经网络模型对这些原始事件进行异常检测，神经网络模型可以如生成式对抗网络模型、长短期记忆网络模型等，神经网络模型可以是预先利用大量的安全事件进行训练后获得的，其可以有效对安全事件进行检测，所以可以通过神经网络模型从原始事件中检测出安全事件，更准确，减少误检的概率。

[0080] 在另一些实施方式中，检测安全事件的方式还可以通过一些异常检测规则对原始事件进行检测，如预先配置异常检测规则，异常检测规则可以是匹配异常的流量特征(如预先设置异常的流量特征)，通过将原始事件的流量特征与异常检测规则进行匹配，匹配上的原始事件即为安全事件。

[0081] 在上述实施例的基础上，为了便于后续对安全事件进行可信度分析，还可以对安全事件进行一些预处理，实现过程如：获取多个初始安全事件，对多个初始安全事件进行标准化形式处理，获得处理后的多个初始安全事件，然后按照预设的过滤规则对处理后的多个初始安全事件进行过滤，获得多个安全事件。

[0082] 其中，多个初始安全事件的获取方式和上述实施例中从原始事件中获取安全事件的方式相同，由于这些安全事件可能来自于不同的设备或应用，形式并不统一，所以，为了便于处理，需要先对这些初始安全事件进行标准化形式处理，处理的方式是将各个初始安全事件转换为具有相同数据格式的事件，也就是说将各个初始安全事件的不同格式的流量特征转换为相同格式的流量特征进行描述，使得其数据格式统一，便于后续进行数据处理。例如，可以预先配置格式化插件，格式化插件是采用特定的语义、特定的格式、用于对安全事件进行格式化的语句的集合，所以可以直接利用格式化插件对各个初始安全事件进行标准化格式处理。

[0083] 为了过滤掉一些不符合要求的安全事件，可以按照预设的过滤规则对处理后获得

的多个初始安全事件进行过滤处理，如预设的过滤规则包括以下至少一项：过滤掉错误或重复的初始安全事件、过滤掉包含内容不全的初始安全事件、过滤掉缺少攻击源或攻击目的地址的初始安全事件。过滤后剩下的多个安全事件即可作为后续进行可信度分析的安全事件，从而可以减少后续过程的处理量。

[0084] 在上述实施例的基础上，在获取与目标历史事件相似的事件集合的方式中，还可以先对多个安全事件进行分类，获得每个安全事件对应的类别，然后对多个安全事件按照事件顺序进行排序，获得事件序列，再根据每个安全事件对应的类别以及事件序列获取与目标历史事件相似的事件集合，其中，事件集合中的安全事件域目标历史事件的类别相同，和/或与目标历史事件发生的时间相近。

[0085] 其中，可以采用贝叶斯分类算法对多个安全事件进行分类，如此可获得每个安全事件对应的类别。分类维度可以包括以下至少一个：来源、目的、协议类型、端口、事件性质等。例如，可以将来源相同的安全事件分为一类，或者将目的相同的安全事件分为一类等。

[0086] 或者，还可以采用K-means聚类算法对多个安全事件进行分类，这样当有新的安全事件产生时，可以直接将其聚类到已有的类别中，以更快速地获得新的安全事件的类别。

[0087] 各个安全事件中可携带有相应的事件发生时间的相关信息，所以可以将多个安全事件按照时间顺序进行排序，这样通过按照时间顺序排序即可获得事件序列。当然，同一时刻发生的安全事件可能有多个。

[0088] 在查找获得事件集合时，可以从多个安全事件中查找与目标历史事件的类别相同的安全事件，如若多个安全事件是按照来源进行分类的，则查找与目标历史事件的来源相同的安全事件作为与目标历史事件相似的安全事件。同理，若是按照其他维度进行分类的，也可以获得与目标历史事件相似的安全事件。举例来说，若目标历史事件A1与安全事件B、C的类别相同，则可认为安全事件B、C为与事件A1相似的安全事件。

[0089] 和/或，还可以获取目标历史事件的发生时间，然后从事件序列中查找与目标历史事件的发生时间相近的安全事件，发生时间相近可以理解为发生时间相同或者发生时间的间隔小于预设时长，如目标历史事件A1的发生时间与某个安全事件D的发生时间的时间间隔小于预设时长，则可认为该安全事件D即为与目标历史事件A1相似的安全事件。

[0090] 所以，通过上述方式可获得与目标历史事件相似的事件集合，如包括事件B、C、D。这样可以找到一些相似的安全事件来对目标安全事件的可信度进行支撑，进而获得更准确的可信度。因为一些安全事件可能有一定的规律，如果发生时间相近或者类别相同，则认为这些安全事件均可能是可信或者均是不可信的，所以，通过分析目标安全事件与这些安全事件之间的关联性，则在一定程度上可以找到更多的信息对目标安全事件的可信度进行支撑，使得目标安全事件的可信度更准确。

[0091] 在上述实施例的基础上，为了便于为后续的安全事件的可信度分析提供数据参考，还可以在获得目标安全事件的可信度之后，根据可信度获取对目标安全事件的可信度分析结果，然后将目标安全事件表中对应的可信度分析结果，并存入历史事件可信度分析结果中。

[0092] 其中，可信度分析结果为是否可信，如若目标安全事件的可信度大于设定值，则目标安全事件的可信度分析结果为可信，反之则不可信，然后将目标安全事件标注对应的可信度分析结果后存入历史事件可信度分析结果中。当然对于多个安全事件中的每个安全事

件也可以按此进行处理，即对每个安全事件均标注对应的可信度分析结果后存入历史事件可信度分析结果中，这样可以积累更多的历史事件可信度分析结果，为后续新的安全事件进行可信度分析提供更多的数据支撑。

[0093] 请参照图3，图3为本申请实施例提供的一种事件可信度分析装置200的结构框图，该装置200可以是电子设备上的模块、程序段或代码。应理解，该装置200与上述图2方法实施例对应，能够执行图2方法实施例涉及的各个步骤，该装置200具体的功能可以参见上文中的描述，为避免重复，此处适当省略详细描述。

[0094] 可选地，所述装置200包括：

[0095] 事件获取模块210，用于获取多个安全事件；

[0096] 历史事件查找模块220，用于针对所述多个安全事件中的目标安全事件，在获得的历史事件可信度分析结果中查找与所述目标安全事件相似的目标历史事件；

[0097] 事件集合获取模块230，用于从所述多个安全事件中获取与所述目标历史事件相似的事件集合，所述事件集合包含至少一个安全事件；

[0098] 可信度计算模块240，用于采用关联分析算法计算获得所述目标安全事件与所述事件集合之间的可信度。

[0099] 可选地，所述事件集合获取模块230，用于对所述多个安全事件进行分类，获得每个安全事件对应的类别；对所述多个安全事件按照时间顺序进行排序，获得事件序列；根据每个安全事件对应的类别以及所述事件序列获取与所述目标历史事件相似的事件集合，其中，所述事件集合中的安全事件与所述目标历史事件的类别相同，和/或与所述目标历史事件发生的时间相近。

[0100] 可选地，所述事件集合获取模块230，用于按照以下至少一个分类维度对所述多个安全事件进行分类，获得每个安全事件对应的类别，所述至少一个分类维度包括：来源、目的、协议类型、端口、事件性质。

[0101] 可选地，所述可信度计算模块240，用于采用Apriori算法计算获得所述目标安全事件的第一支持度以及所述目标安全事件与所述事件集合的第二支持度；根据所述第一支持度以及所述第二支持度计算获得所述目标安全事件与所述事件集合之间的可信度。

[0102] 可选地，所述装置200还包括：

[0103] 存储模块，用于根据所述可信度获取对所述目标安全事件的可信度分析结果；将所述目标安全事件标注对应的可信度分析结果，并存入所述历史事件可信度分析结果中。

[0104] 可选地，所述事件获取模块210，用于获取原始事件；采用神经网络模型对所述原始事件进行异常检测，获得多个安全事件。

[0105] 可选地，所述事件获取模块210，用于获取多个初始安全事件；对所述多个初始安全事件进行标准化形式处理，获得处理后的多个初始安全事件；按照预设的过滤规则对所述处理后的多个初始安全事件进行过滤，获得多个安全事件。

[0106] 需要说明的是，本领域技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的装置的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再重复描述。

[0107] 本申请实施例提供一种可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时，执行如图2所示方法实施例中电子设备所执行的方法过程。

[0108] 本实施例公开一种计算机程序产品，所述计算机程序产品包括存储在非暂态计算

机可读存储介质上的计算机程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，计算机能够执行上述各方法实施例所提供的方法，例如，包括：获取多个安全事件；针对所述多个安全事件中的目标安全事件，在获得的历史事件可信度分析结果中查找与所述目标安全事件相似的目标历史事件；从所述多个安全事件中获取与所述目标历史事件相似的事件集合，所述事件集合包含至少一个安全事件；采用关联分析算法计算获得所述目标安全事件与所述事件集合之间的可信度。

[0109] 综上所述，本申请实施例提供一种事件可信度分析方法、装置、电子设备及可读存储介质，该方法在对目标安全事件进行分析时，从历史事件可信度分析结果中查找与其相似的目标历史事件，然后获取与目标历史事件相似的事件结合，并利用关联分析算法计算获得目标安全事件与事件集合之间的可信度，以获得目标安全事件的可信度，无需通过人工识别，效率更高。并且，通过结合历史事件可信度分析结果，对安全事件的可信度分析提供一定程度上的数据支撑，使得分析结果更准确。

[0110] 在本申请所提供的实施例中，应该理解到，所揭露装置和方法，可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，又例如，多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些通信接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0111] 另外，作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0112] 再者，在本申请各个实施例中的各功能模块可以集成在一起形成一个独立的部分，也可以是各个模块单独存在，也可以两个或两个以上模块集成形成一个独立的部分。

[0113] 在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。

[0114] 以上所述仅为本申请的实施例而已，并不用于限制本申请的保护范围，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

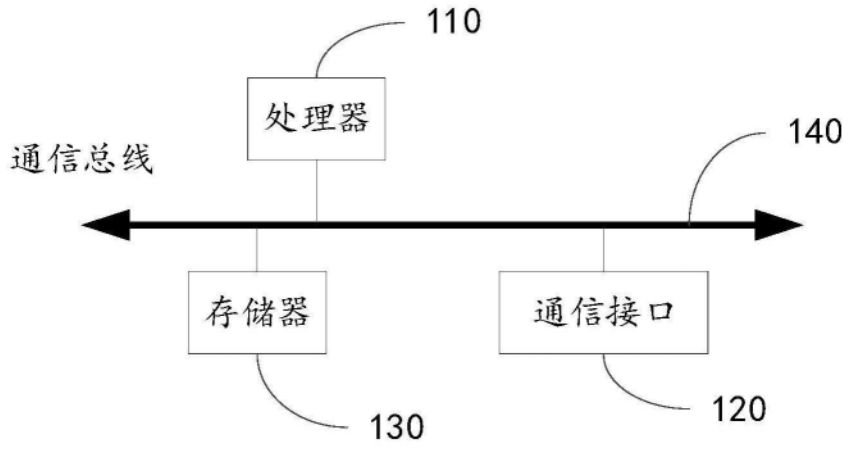

110
处理器
通信总线
140
存储器
通信接口
130
120

图1

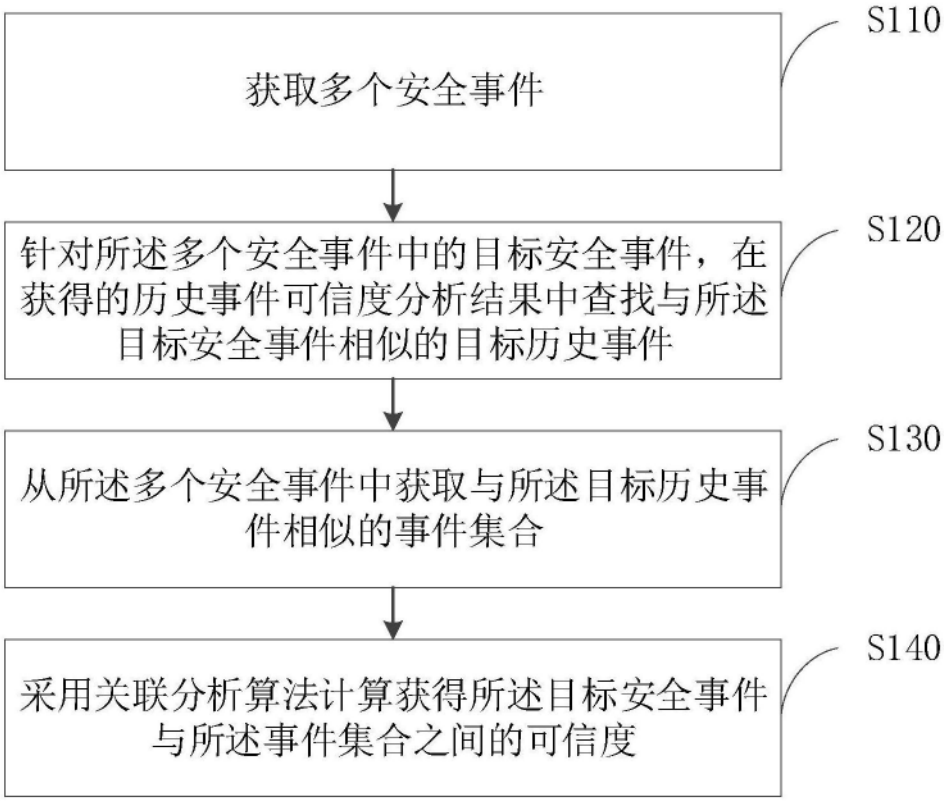

S110
获取多个安全事件
S120
针对所述多个安全事件中的目标安全事件，在获得的历史事件可信度分析结果中查找与所述目标安全事件相似的目标历史事件
S130
从所述多个安全事件中获取与所述目标历史事件相似的事件集合
S140
采用关联分析算法计算获得所述目标安全事件与所述事件集合之间的可信度

图2

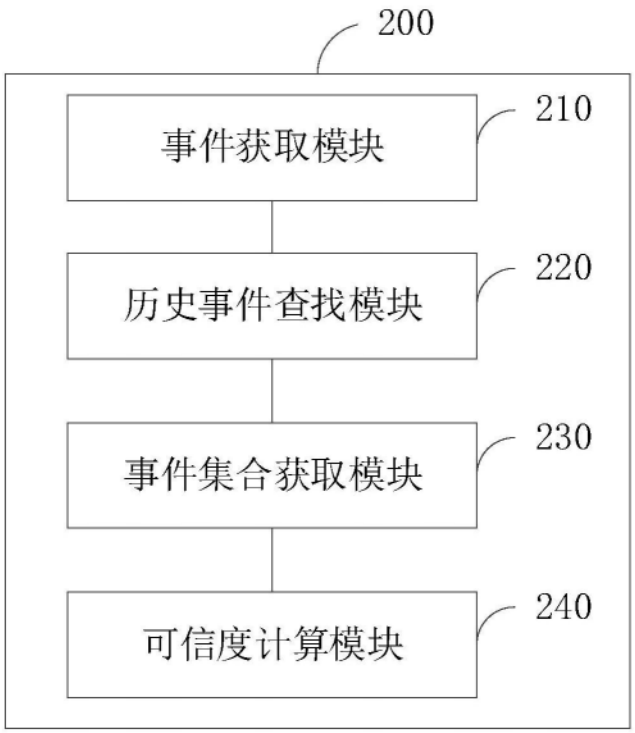



图3