(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 113965356 A
(43)申请公布日 2022.01.21

(21)申请号 202111142145.1

(22)申请日 2021.09.28

(71)申请人 新华三信息安全技术有限公司
地址 230001 安徽省合肥市高新区创新大道2800号创新产业园二期H2栋541室

(72)发明人 顾涛 金兆岩 赵志伟

(51)Int.Cl.
H04L 9/40(2022.01)

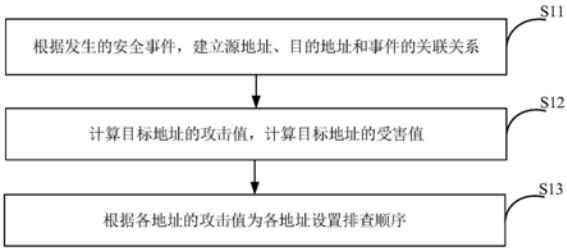
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种安全事件分析方法、装置、设备及机器可读存储介质

(57)摘要

本公开提供一种安全事件分析方法、装置、设备及机器可读存储介质，该方法包括：根据发生的安全事件，建立源地址、目的地址和事件的关联关系；计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值；计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值；根据各地址的攻击值为各地址设置排查顺序。通过本公开的技术方案，利用风险资产对应的地址，根据关联的其他地址的受害值和攻击值得到风险资产对应地址的攻击值和受害值，然后根据可量化的数值为各风险资产对应的地址排序，得到风险资产的排查顺序，提高运维效率。



CN 113965356 A

1.一种安全事件分析方法,其特征在于,应用于网络安全设备,所述方法包括:

根据发生的安全事件,建立源地址、目的地址和事件的关联关系,以源地址作为攻击者具有攻击值,以目的地址作为受害者具有受害值;

计算目标地址的攻击值,所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值;

计算目标地址的受害值,所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值;

根据各地址的攻击值为各地址设置排查顺序。

2.根据权利要求1所述的方法,其特征在于,根据关联的受害值,为攻击值相同的地址设置排查顺序。

3.根据权利要求1所述的方法,其特征在于,所述计算目标地址的攻击值,所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值,计算目标地址的受害值,所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值,包括:

每次迭代,根据更新的关联的受害值重新计算攻击值,根据更新的关联的攻击值重新计算受害值,在迭代次数达到预设次数后,停止迭代。

4.根据权利要求1所述的方法,其特征在于,

所述根据发生的安全事件,建立源地址、目的地址和事件的关联关系,以源地址作为攻击者具有攻击值,以目的地址作为受害者具有受害值,包括:

根据发生的安全事件,建立源地址、目的地址和事件权重的关联关系;

所述计算目标地址的攻击值,所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值,包括:

所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值及安全事件对应的权重;

所述计算目标地址的受害值,所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值,包括:

所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值及安全事件对应的权重。

5.一种安全事件分析装置,其特征在于,应用于网络安全设备,所述装置包括:

关联模块,用于根据发生的安全事件,建立源地址、目的地址和事件的关联关系,以源地址作为攻击者具有攻击值,以目的地址作为受害者具有受害值;

计算模块,用于计算目标地址的攻击值,所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值;

计算模块还用于计算目标地址的受害值,所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值;

排序模块,用于根据各地址的攻击值为各地址设置排查顺序。

6.根据权利要求5所述的装置,其特征在于,根据关联的受害值,为攻击值相同的地址设置排查顺序。

7.根据权利要求5所述的装置,其特征在于,所述计算目标地址的攻击值,所述目标地

址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值，计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值，包括：

每次迭代，根据更新的关联的受害值重新计算攻击值，根据更新的关联的攻击值重新计算受害值，在迭代次数达到预设次数后，停止迭代。

8.根据权利要求5所述的装置，其特征在于，

所述根据发生的安全事件，建立源地址、目的地址和事件的关联关系，以源地址作为攻击者具有攻击值，以目的地址作为受害者具有受害值，包括：

根据发生的安全事件，建立源地址、目的地址和事件权重的关联关系；

所述计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值，包括：

所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值及安全事件对应的权重；

所述计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值，包括：

所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值及安全事件对应的权重。

9.一种电子设备，其特征在于，包括：处理器和机器可读存储介质，所述机器可读存储介质存储有能够被所述处理器执行的机器可执行指令，所述处理器执行所述机器可执行指令，以实现权利要求1-4任一所述的方法。

10.一种机器可读存储介质，其特征在于，所述机器可读存储介质存储有机器可执行指令，所述机器可执行指令在被处理器调用和执行时，所述机器可执行指令促使所述处理器实现权利要求1-4任一所述的方法。

一种安全事件分析方法、装置、设备及机器可读存储介质

技术领域

[0001] 本公开涉及通信技术领域，尤其是涉及一种安全事件分析方法、装置、设备及机器可读存储介质。

背景技术

[0002] 安全管理平台(包括不限于态势感知，SOC，SIME等)是以安全大数据为基础，对能够引起网络态势发生变化的要素进行获取、理解、评估、呈现以及对未来发展趋势进行预测。以全局视角提升对安全威胁的发现识别、理解分析、响应处置的能力，通过智能分析和联动响应，结合机器学习和人工智能，推动安全大脑的闭环决策，实现安全能力的落地实践。

[0003] 其中，上报到安全管理平台的安全告警是安全管理平台分析的基础，如果上报了成千上万条安全告警，将会给安全运维人员排查处置带来巨大的工作压力。当前安全运维人员可以通过风险资产的威胁等级，已失陷，高可疑，低可疑等定性的方法去排查失陷等级较高的资产。但是，如果出现了大量相同威胁等级的风险资产，安全运维人员就只好逐个排查分析，从而排查效率低。

发明内容

[0004] 有鉴于此，本公开提供一种安全事件分析方法、装置及电子设备、机器可读存储介质，以改善上述存在大量同威胁等级的风险资产时排查效率低的问题。

[0005] 具体地技术方案如下：

[0006] 本公开提供了一种安全事件分析方法，应用于网络安全设备，所述方法包括：根据发生的安全事件，建立源地址、目的地址和事件的关联关系，以源地址作为攻击者具有攻击值，以目的地址作为受害者具有受害值；计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值；计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值；根据各地址的攻击值为各地址设置排查顺序。

[0007] 作为一种技术方案，根据关联的受害值，为攻击值相同的地址设置排查顺序。

[0008] 作为一种技术方案，所述计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值，计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值，包括：每次迭代，根据更新的关联的受害值重新计算攻击值，根据更新的关联的攻击值重新计算受害值，在迭代次数达到预设次数后，停止迭代。

[0009] 作为一种技术方案，所述根据发生的安全事件，建立源地址、目的地址和事件的关联关系，以源地址作为攻击者具有攻击值，以目的地址作为受害者具有受害值，包括：根据发生的安全事件，建立源地址、目的地址和事件权重的关联关系；所述计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受

害值，包括：所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值及安全事件对应的权重；所述计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值，包括：所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值及安全事件对应的权重。

[0010] 本公开同时提供了一种安全事件分析装置，应用于网络安全设备，所述装置包括：关联模块，用于根据发生的安全事件，建立源地址、目的地址和事件的关联关系，以源地址作为攻击者具有攻击值，以目的地址作为受害者具有受害值；计算模块，用于计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值；计算模块还用于计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值；排序模块，用于根据各地址的攻击值为各地址设置排查顺序。

[0011] 作为一种技术方案，根据关联的受害值，为攻击值相同的地址设置排查顺序。

[0012] 作为一种技术方案，所述计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值，计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值，包括：每次迭代，根据更新的关联的受害值重新计算攻击值，根据更新的关联的攻击值重新计算受害值，在迭代次数达到预设次数后，停止迭代。

[0013] 作为一种技术方案，所述根据发生的安全事件，建立源地址、目的地址和事件的关联关系，以源地址作为攻击者具有攻击值，以目的地址作为受害者具有受害值，包括：根据发生的安全事件，建立源地址、目的地址和事件权重的关联关系；所述计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值，包括：所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值及安全事件对应的权重；所述计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值，包括：所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值及安全事件对应的权重。

[0014] 本公开同时提供了一种电子设备，包括处理器和机器可读存储介质，所述机器可读存储介质存储有能够被所述处理器执行的机器可执行指令，处理器执行所述机器可执行指令以实现前述的安全事件分析方法。

[0015] 本公开同时提供了一种机器可读存储介质，所述机器可读存储介质存储有机器可执行指令，所述机器可执行指令在被处理器调用和执行时，所述机器可执行指令促使所述处理器实现前述的安全事件分析方法。

[0016] 本公开提供的上述技术方案至少带来了以下有益效果：

[0017] 利用风险资产对应的地址，根据关联的其他地址的受害值和攻击值得到风险资产对应地址的攻击值和受害值，然后根据可量化的数值为各风险资产对应的地址排序，得到风险资产的排查顺序，提高运维效率。

附图说明

[0018] 为了更加清楚地说明本公开实施方式或者现有技术中的技术方案，下面将对本公开实施方式或者现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本公开中记载的一些实施方式，对于本领域普通技术人员来讲，还可以根据本公开实施方式的这些附图获得其他的附图。

[0019] 图1是本公开一种实施方式中的安全事件分析方法的流程图；

[0020] 图2是本公开一种实施方式中的安全事件分析装置的结构图；

[0021] 图3是本公开一种实施方式中的电子设备的硬件结构图。

具体实施方式

[0022] 在本公开实施方式使用的术语仅仅是出于描述特定实施方式的目的，而非限制本公开。本公开和权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其它含义。还应当理解，本文中使用的术语“和/或”是指包含一个或多个相关联的列出项目的任何或所有可能组合。

[0023] 应当理解，尽管在本公开实施方式可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本公开范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，此外，所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0024] 本公开提供一种安全事件分析方法、装置及电子设备、机器可读存储介质，以改善上述存在大量同威胁等级的风险资产时排查效率低的问题。

[0025] 具体地，技术方案如后述。

[0026] 在一种实施方式中，本公开提供了一种安全事件分析方法，应用于网络安全设备，所述方法包括：根据发生的安全事件，建立源地址、目的地址和事件的关联关系，以源地址作为攻击者具有攻击值，以目的地址作为受害者具有受害值；计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值；计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值；根据各地址的攻击值为各地址设置排查顺序。

[0027] 具体地，如图1，包括以下步骤：

[0028] 步骤S11，根据发生的安全事件，建立源地址、目的地址和事件的关联关系；

[0029] 以源地址作为攻击者具有攻击值，以目的地址作为受害者具有受害值。

[0030] 步骤S12，计算目标地址的攻击值，计算目标地址的受害值；

[0031] 所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值。

[0032] 步骤S13，根据各地址的攻击值为各地址设置排查顺序。

[0033] 利用风险资产对应的地址，根据关联的其他地址的受害值和攻击值得到风险资产对应地址的攻击值和受害值，然后根据可量化的数值为各风险资产对应的地址排序，得到风险资产的排查顺序，提高运维效率。

[0034] 在一种实施方式中，根据关联的受害值，为攻击值相同的地址设置排查顺序。

[0035] 在一种实施方式中，所述计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值，计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值，包括：每次迭代，根据更新的关联的受害值重新计算攻击值，根据更新的关联的攻击值重新计算受害值，在迭代次数达到预设次数后，停止迭代。

[0036] 在一种实施方式中，所述根据发生的安全事件，建立源地址、目的地址和事件的关联关系，以源地址作为攻击者具有攻击值，以目的地址作为受害者具有受害值，包括：根据发生的安全事件，建立源地址、目的地址和事件权重的关联关系；所述计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值，包括：所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值及安全事件对应的权重；所述计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值，包括：所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值及安全事件对应的权重。

[0037] 在一种实施方式中，基于spark graphx等图计算引擎将可信安全事件添加到图中，点是源IP地址和目的IP地址，连接源IP地址和目的IP地址的作为边是事件权重。其中事件权重关联于事件最近发生时间、事件发生的次数和事件的威胁程度，还可以加入其它需要的属性。

[0038] 针对特殊事件，如多条事件聚合成一条事件，对源IP地址或目的IP地址，转换成【源IP＝0.0.0.0】和【目的IP＝255.255.255.255】。多对一聚合事件如外网DDoS攻击内网资产，源IP表示成0.0.0.0。一对多聚合事件如蠕虫内网传播，目的IP表示成255.255.255.255。

[0039] 任意节点的地址(风险资产对应)具有两个属性，攻击值HUB和受害值AUT，该地址的攻击值关联于所有以地址作为源地址的节点的受害值之和，该地址的受害值关联于所有以地址作为目的地址的节点的攻击值之和。一种计算方法中，根据AUT计算HUB时，加入各事件关联的权重值，以各AUT分别乘以关联的各权重值后，求和得到HUB；一种计算方法中，根据HUB计算AUT时，加入各事件关联的权重值，以各HUB分别乘以关联的各权重值后，求和得到AUT。其中事件的权重值关联于事件的预先配置的威胁等级、发生的次数以及最近一次发生的时间，威胁等级越高则权重值越大，发生次数越多则权重值越大，最近一次发生的时间越近则权重值越大。

[0040] 由于某一地址的HUB变化后，与之关联的地址的AUT随之应该发生变化，进而该地址的HUB应应当随着与之关联的地址的AUT变化后变化，因而此处进行迭代计算。迭代次数设置上限，如100次等，正常情况下，在迭代次数达到上限前，各HUB和AUT达到稳态。为了防止迭代过拟合，当第二高HUB是最高HUB的40％或更高时，应当停止迭代。

[0041] 根据关联的HUB值，为各地址排序，优先排查关联的地址排序高的风险资产，当HUB值相同时，以AUT值进行二次排序。

[0042] 在一种实施方式中，本公开同时提供了一种安全事件分析装置，如图2，应用于网络安全设备，所述装置包括：关联模块21，用于根据发生的安全事件，建立源地址、目的地址

和事件的关联关系，以源地址作为攻击者具有攻击值，以目的地址作为受害者具有受害值；计算模块22，用于计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值；计算模块还用于计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值；排序模块23，用于根据各地址的攻击值为各地址设置排查顺序。

[0043] 在一种实施方式中，根据关联的受害值，为攻击值相同的地址设置排查顺序。

[0044] 在一种实施方式中，所述计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值，计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值，包括：每次迭代，根据更新的关联的受害值重新计算攻击值，根据更新的关联的攻击值重新计算受害值，在迭代次数达到预设次数后，停止迭代。

[0045] 在一种实施方式中，所述根据发生的安全事件，建立源地址、目的地址和事件的关联关系，以源地址作为攻击者具有攻击值，以目的地址作为受害者具有受害值，包括：根据发生的安全事件，建立源地址、目的地址和事件权重的关联关系；所述计算目标地址的攻击值，所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值，包括：所述目标地址的攻击值关联于所有以目标地址作为源地址的安全事件的目的地址的受害值及安全事件对应的权重；所述计算目标地址的受害值，所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值，包括：所述目标地址的受害值关联于所有以目标地址作为目的地址的安全事件的源地址的攻击值及安全事件对应的权重。

[0046] 装置实施方式与对应的方法实施方式相同或相似，在此不再赘述。

[0047] 在一种实施方式中，本公开提供了一种电子设备，包括处理器和机器可读存储介质，所述机器可读存储介质存储有能够被所述处理器执行的机器可执行指令，处理器执行所述机器可执行指令以实现前述的安全事件分析方法，从硬件层面而言，硬件架构示意图可以参见图3所示。

[0048] 在一种实施方式中，本公开提供了一种机器可读存储介质，所述机器可读存储介质存储有机器可执行指令，所述机器可执行指令在被处理器调用和执行时，所述机器可执行指令促使所述处理器实现前述的安全事件分析方法。

[0049] 这里，机器可读存储介质可以是任何电子、磁性、光学或其它物理存储装置，可以包含或存储信息，如可执行指令、数据，等等。例如，机器可读存储介质可以是：RAM(Radom Access Memory，随机存取存储器)、易失存储器、非易失性存储器、闪存、存储驱动器(如硬盘驱动器)、固态硬盘、任何类型的存储盘(如光盘、dvd等)，或者类似的存储介质，或者它们的组合。

[0050] 上述实施方式阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[0051] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本

公开时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0052] 本领域内的技术人员应明白，本公开的实施方式可提供为方法、系统、或计算机程序产品。因此，本公开可采用完全硬件实施方式、完全软件实施方式、或结合软件和硬件方面的实施方式的形式。而且，本公开实施方式可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0053] 本公开是参照根据本公开实施方式的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可以由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其它可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其它可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0054] 而且，这些计算机程序指令也可以存储在能引导计算机或其它可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或者多个流程和/或方框图一个方框或者多个方框中指定的功能。

[0055] 这些计算机程序指令也可装载到计算机或其它可编程数据处理设备上，使得在计算机或者其它可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其它可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0056] 本领域技术人员应明白，本公开的实施方式可提供为方法、系统或计算机程序产品。因此，本公开可以采用完全硬件实施方式、完全软件实施方式、或者结合软件和硬件方面的实施方式的形式。而且，本公开可以采用在一个或者多个其中包含有计算机可用程序代码的计算机可用存储介质(可以包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0057] 以上所述仅为本公开的实施方式而已，并不用于限制本公开。对于本领域技术人员来说，本公开可以有各种更改和变化。凡在本公开的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本公开的权利要求范围之内。

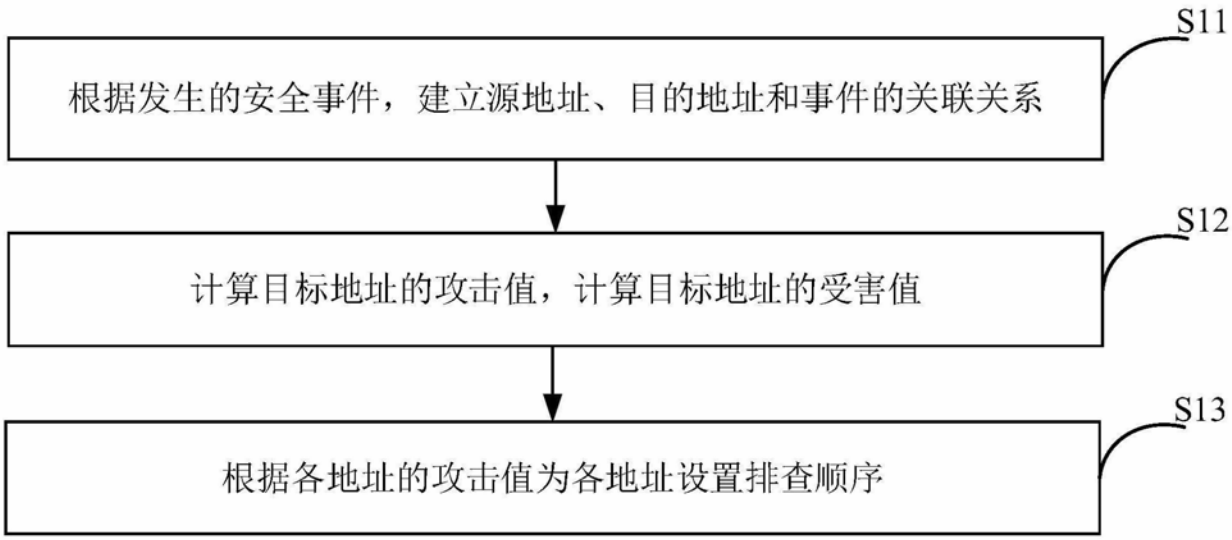

S11
根据发生的安全事件，建立源地址、目的地址和事件的关联关系
S12
计算目标地址的攻击值，计算目标地址的受害值
S13
根据各地址的攻击值为各地址设置排查顺序

图1

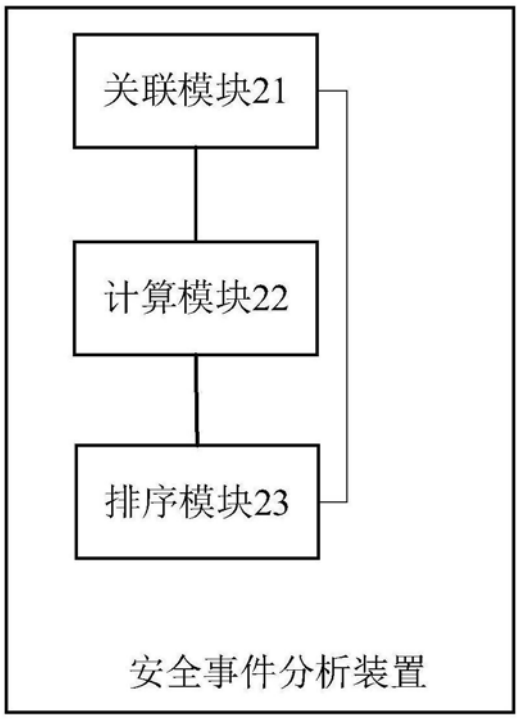

关联模块21
计算模块22
排序模块23
安全事件分析装置

图2

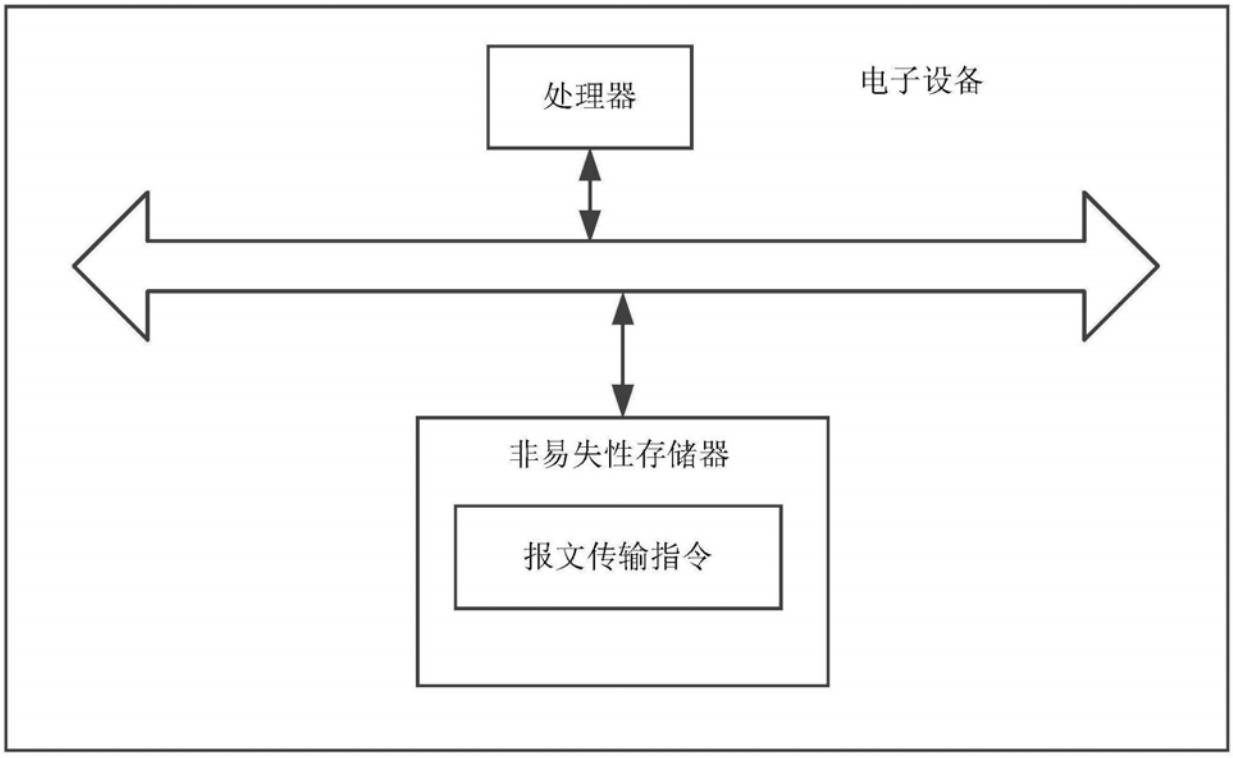


图3