(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110620759 B
(45)授权公告日 2023.05.16

(21)申请号 201910636986.4
(22)申请日 2019.07.15
(65)同一申请的已公布的文献号
申请公布号 CN 110620759 A
(43)申请公布日 2019.12.27
(73)专利权人 公安部第一研究所
地址 100044 北京市海淀区首都体育馆南路1号
专利权人 北京中盾安全技术开发公司
(72)发明人 栗红梅 黄小平 孟博 常玉兰 陈朝武 郑裕林 闫雪 张振环 柳娜
(74)专利代理机构 北京汲智翼成知识产权代理事务所(普通合伙) 11381
专利代理师 陈曦 贾兴昌
(51)Int.Cl.
H04L 9/40(2022.01)
G06F 21/57(2013.01)

(56)对比文件
CN 107995162 A,2018.05.04
CN 109246153 A,2019.01.18
CN 103748999 B,2012.02.08
章翔凌等.基于大数据分析的应用安全态势系统设计与实现.《网络空间安全》.2017,全文.
吴华等.大规模网络安全事件威胁量化分析.《微计算机信息》.2008,(第09期),全文.
任俊等.基于G1-层次分析法信息系统风险等级评估研究.《电脑知识与技术》.2018,(第09期),全文.
黄亮亮.网络安全态势评估与预测方法的研究.《中国优秀硕士学位论文全文数据库 信息科技辑》.2016,

审查员 冯婕

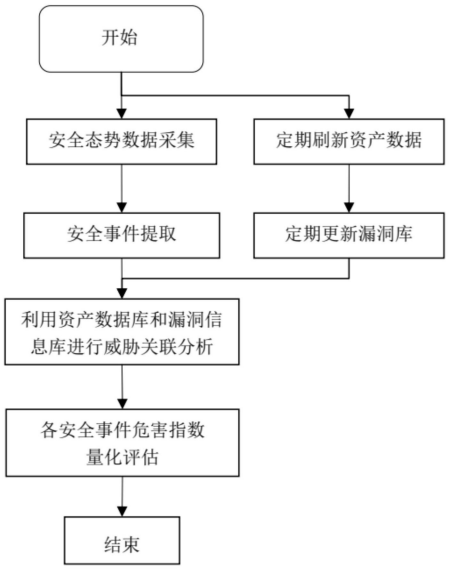
权利要求书2页 说明书8页 附图6页

(54)发明名称

基于多维关联的网络安全事件危害指数评估方法及其系统

(57)摘要

本发明公开了一种基于多维关联的网络安全事件危害指数评估方法,同时也公开了采用该网络安全事件危害指数评估方法的网络安全态势感知系统。该方法建立在资产数据库和漏洞数据库的基础上,利用威胁建模测算出攻击事件对安全网络造成的危害,然后针对特定的威胁攻击给安全系统带来的威胁进行量化,考虑影响网络安全的因素包括安全事件、主机漏洞以及提供的服务等,并根据安全活动与资产、漏洞等对应关系,分析这些活动的危害程度,评估的结果更加准确和可信。



CN 110620759 B

1.一种基于多维关联的网络安全事件危害指数评估方法,其特征在于包括如下步骤:

采集网络安全态势数据并提取安全事件;同时,定期刷新资产数据并定期更新漏洞数据库;

利用资产数据库和漏洞数据库进行威胁关联分析;

对各个网络安全事件危害指数进行量化评估;其中,所述网络安全事件危害指数是与成本、权重和命中率相关的函数,并且通过下式进行计算:

$Host=\sum H_i*Q_i*M_i+\sum Q_j*Q_j*M_j+\sum R_k*Q_k*M_k+\sum S_l*Q_l*M_l$

$Sys=\sum Host_m$

其中,$Host_m$代表网络安全事件对某个主机造成的危害指数,Sys代表在本监测系统内网络安全事件的危害指数,H_i代表硬件的成本指数,O_j代表操作系统的成本指数,R_k代表组件的成本指数,S_l代表服务的成本指数,Q代表该类网络安全事件造成危害和影响的权重,M代表网络安全事件是否命中目标。

2.如权利要求1所述的网络安全事件危害指数评估方法,其特征在于:

利用网络资产识别技术及工具收集网络系统内的资产数据,形成并定期刷新资产数据库。

3.如权利要求1所述的网络安全事件危害指数评估方法,其特征在于:

所述漏洞数据库不限于本地网络系统采集的内容,也包括在互联网中采集的漏洞数据。

4.如权利要求1所述的网络安全事件危害指数评估方法,其特征在于:

在所述网络安全态势数据的采集过程中,不断提取网络安全事件。

5.如权利要求1所述的网络安全事件危害指数评估方法,其特征在于所述威胁关联分析包括如下内容:

1)通过网络安全事件的目的IP,在资产数据库中查找与该IP地址匹配的主机;

2)在资产数据库中,查找主机所拥有的资源情况,这些资源包括硬件、操作系统、软件和服务、网络带宽使用量;

3)在漏洞数据库中,对可能受到漏洞影响的组件的各项指标进行赋值。

6.一种网络安全态势感知系统,包括安全响应与策略配置单元、安全关联分析单元、安全事件统计分析单元、网络安全事件危害指数量化单元和安全态势评估单元;其中,

所述网络安全事件危害指数量化单元分别从安全响应与策略配置单元、安全关联分析单元、安全事件统计分析单元中获取数据,以执行权利要求1～5中任意一项所述的网络安全事件危害指数评估方法;

所述网络安全事件危害指数量化单元与所述安全态势评估单元之间交互数据。

7.如权利要求6所述的网络安全态势感知系统,其特征在于还包括安全数据采集单元、数据库、知识库以及管理支撑子系统;其中,

所述安全数据采集单元分别向所述安全响应与策略配置单元、所述安全关联分析单元和所述安全事件统计分析单元提供所采集的基础安全数据。

8.如权利要求6所述的网络安全态势感知系统,其特征在于通过如下步骤执行权利要求1～5中任意一项所述的网络安全事件危害指数评估方法:

步骤1:安全态势数据采集;

步骤2:数据预处理及其安全事件鉴别;

步骤3:威胁关联分析;

步骤4:指标定义及其危害指数评定;

步骤5:指标合成及安全总体指数综合评价;

步骤6:进行整体网络安全态势的评估;

步骤7:展示安全态势。

基于多维关联的网络安全事件危害指数评估方法及其系统

技术领域

[0001] 本发明涉及一种网络安全评估方法，尤其涉及一种基于多维关联的网络安全事件危害指数评估方法，同时也涉及采用该网络安全事件危害指数评估方法的网络安全态势感知系统，属于网络安全技术领域。

背景技术

[0002] 当前，全球的网络安全环境和形势已经发生了深刻的变化，所要解决的主要问题是：当攻击者发起攻击，安全事件发生时，能不能在最短的时间内发现和预警，能不能有时间准备和处置。网络安全态势感知作为一种主动的网络防御技术手段，不仅能够反映当前的网络安全态势，并且能够对网络中潜在的攻击做出预测，从而对潜在攻击做出主动防御。

[0003] 在现有技术中，网络安全态势感知系统普遍是基于日志采集、大数据分析及预测等技术手段实现的，具有滞后性，缺少对网络漏洞造成危害具有针对性的评估方法和手段。同时，因网络入侵行为逐渐趋于复杂化和间接化，现有的态势预测理论或算法存在主观化、评估不够准确，以及使用条件苛刻等方面的不足，尤其是当网络过于复杂，数据量迅猛发展的当前，评估效率显得尤为低下。如何避免上述缺陷，能够在特定应用场景下，准确、方便、高效地评估网络存在的风险，成为亟须解决的技术课题。

[0004] 在公开号为CN106341414A的中国专利申请中，公开了一种基于贝叶斯网络的多步攻击安全态势评估方法。该方法通过关联分析挖掘多步攻击发生模式构建攻击图，根据多步攻击图建立贝叶斯网络，将攻击意愿、攻击成功概率、事件监测正确率定义为贝叶斯网络概率属性；结合事件监测，通过贝叶斯网络后验推理和累积概率计算多步攻击风险。另外，在公开号为CN101783752A的中国专利申请中，也公开了一种基于网络拓扑特征的网络安全量化评估方法。该方法通过选取用于评估网络安全事件损害程度的网络性能指标，定义网络熵值和计算每一个网络性能指标的指标权重，利用格兰姆施密特正交化方法去除多个网络性能指标间的相关性，获得多个去相关网络性能指标，从而获得安全事件损害程度和安全事件损害等级，通过量化网络拓扑特征评估网络安全事件对网络性能的影响程度。

[0005] 但是，以上述专利申请为代表的现有技术所存在的问题是：缺乏真正意义上的联动互操作能力和基于各种日志的综合交叉分析能力。由于缺乏较科学的定性和定量相结合的分析手段，导致无法准确评估安全事件的威胁程度，提不出切实可行的应急防范措施，无法胜任安全预警的任务和目标。

发明内容

[0006] 本发明所要解决的首要技术问题在于提供一种基于多维关联的网络安全事件危害指数评估方法。

[0007] 本发明所要解决的另一技术问题在于提供一种采用该网络安全事件危害指数评估方法的网络安全态势感知系统。

[0008] 为实现上述发明目的，本发明采用下述的技术方案：

[0009] 根据本发明实施例的第一方面，提供一种基于多维关联的网络安全事件危害指数评估方法，包括如下步骤：

[0010] ⑴安全态势数据采集；

[0011] ⑵安全事件提取；

[0012] ⑶利用资产数据库和漏洞数据库进行威胁关联分析；

[0013] ⑷对各个网络安全事件危害指数进行量化评估；其中，

[0014] 在所述安全态势数据采集和所述安全事件提取步骤进行的同时，定期刷新资产数据并定期更新漏洞数据库。

[0015] 其中较优地，利用网络资产识别技术及工具收集网络系统内的资产数据，形成并定期刷新资产数据库。

[0016] 其中较优地，所述漏洞数据库不限于本地网络系统采集的内容，也包括在互联网中采集的漏洞数据。

[0017] 其中较优地，所述步骤⑵中，从网络安全态势数据的采集过程中不断提取出网络安全事件。

[0018] 其中较优地，所述步骤⑶中，所述威胁关联分析包括如下内容：

[0019] 1)通过网络安全事件的目的IP，在资产数据库中查找与该IP地址匹配的主机；

[0020] 2)在资产数据库中，查找主机所拥有的资源情况，这些资源包括硬件、操作系统、软件和服务、网络带宽使用量；

[0021] 3)在漏洞数据库中，对可能受到漏洞影响的组件的各项指标进行赋值。

[0022] 其中较优地，所述步骤⑷中，所述网络安全事件危害指数是与成本、权重和命中率相关的函数。

[0023] 其中较优地，所述网络安全事件危害指数通过下式进行计算：

[0024] $Host=\sum H_i*Q_i*M_i+\sum Q_j*Q_j*M_j+\sum R_k*Q_k*M_k+\sum S_l*Q_l*M_l$

[0025] $Sys=\sum Host_m$

[0026] 其中，$Host_m$代表网络安全事件对某个主机造成的危害指数，Sys代表在本监测系统内网络安全事件的危害指数，H_i代表硬件的成本指数，O_j代表操作系统的成本指数，R_k代表组件的成本指数，S_l代表服务的成本指数，Q代表该类网络安全事件造成危害和影响的权重，M代表网络安全事件是否命中目标。

[0027] 根据本发明实施例的第二方面，提供一种网络安全态势感知系统，包括安全响应与策略配置单元、安全关联分析单元、安全事件统计分析单元、网络安全事件危害指数量化单元和安全态势评估单元；其中，

[0028] 所述网络安全事件危害指数量化单元分别从安全响应与策略配置单元、安全关联分析单元、安全事件统计分析单元中获取数据，以执行上述的网络安全事件危害指数评估方法；

[0029] 所述网络安全事件危害指数量化单元与所述安全态势评估单元之间交互数据。

[0030] 其中较优地，还包括安全数据采集单元、数据库、知识库以及管理支撑子系统；其中，

[0031] 所述安全数据采集单元分别向所述安全响应与策略配置单元、所述安全关联分析单元和所述安全事件统计分析单元提供所采集的基础安全数据。

[0032] 其中较优地，通过如下步骤执行上述的网络安全事件危害指数评估方法：

[0033] 步骤1：安全态势数据采集；

[0034] 步骤2：数据预处理及其安全事件鉴别；

[0035] 步骤3：威胁关联分析；

[0036] 步骤4：指标定义及其危害指数评定；

[0037] 步骤5：指标合成及安全总体指数综合评价；

[0038] 步骤6：进行整体网络安全态势的评估；

[0039] 步骤7：安全态势展示。

[0040] 与现有技术相比较，本发明是建立在资产数据库和漏洞数据库基础上的网络安全态势量化评估方法，利用威胁建模测算出攻击事件对安全网络造成的危害，然后针对特定的威胁攻击给安全系统带来的威胁进行量化，考虑影响网络安全的因素包括安全事件、主机漏洞以及提供的服务等，并根据安全活动与资产、漏洞等对应关系，分析这些活动的危害程度，评估的结果更加准确和可信。

附图说明

[0041] 图1为本发明所提供的网络安全事件危害指数评估方法的流程图；

[0042] 图2为当前网络环境下，黑客攻击事件的示意图；

[0043] 图3为针对黑客攻击事件进行安全巡查，发现风险并产生预警的示意图；

[0044] 图4为本发明所提供的网络安全态势感知系统的示意图；

[0045] 图5为网络安全态势感知系统执行网络安全事件危害指数评估方法的流程图；

[0046] 图6为网络安全态势综合感知体系的逻辑架构示意图。

具体实施方式

[0047] 下面结合附图和具体实施例对本发明的技术内容做进一步的详细说明。

[0048] 针对现有技术所存在的不足，本发明首先提供一种客观的安全态势评测方法。该方法是建立在资产数据库和漏洞数据库基础上的网络安全态势量化评估方法，利用威胁建模测算出攻击事件对安全网络造成的危害，然后针对特定的威胁攻击给安全系统带来的威胁进行量化评估。由于该方法综合考虑了影响网络安全的因素包括安全事件、主机漏洞以及提供的服务等，并根据安全活动与资产、漏洞等对应关系，分析这些活动的危害程度，评估的结果更加准确和可信。

[0049] 图1为本发明所提供的网络安全事件危害指数评估方法的流程图。参见图1所示，该方法主要包括安全态势数据采集、安全事件提取、利用资产数据库和漏洞数据库进行威胁关联分析、对各个网络安全事件危害指数进行量化评估等步骤。其中，在安全态势数据采集和安全事件提取步骤进行的同时，定期刷新资产数据并定期更新漏洞数据库。下面对上述各步骤的具体实施过程展开详细说明。

[0050] 1.安全态势数据采集

[0051] 安全态势数据采集为网络安全态势感知提出基础数据源，是网络安全事件危害指数评估方法的第一步。在本发明的一个实施例中，可以通过定制数据采集的代理，同时支持主动收集及被动接收的数据采集方式。例如，采用Snmp和Syslog收集网络流量信息、日志信

息等,通过配置不同的网络安全设备,从而完成对各类安全态势数据的采集。

[0052] 2.安全事件提取

[0053] 从网络安全态势数据(包含安全监测日志)的采集过程中不断提取出网络安全事件(即网络攻击事件)。由于网络态势感知的数据来自众多的网络设备,表达的语义也不尽相同,其数据格式、数据内容和数据质量千差万别,需要经过数据预处理和分类归并后才能形成可利用的网络安全事件。

[0054] 在上述安全态势数据采集和安全事件提取步骤进行的同时,利用网络资产识别技术及工具收集网络系统内的资产数据,形成并定期刷新资产数据库。在本发明中,网络内的资产数据以主机为单位建立资产数据体系,主机类型包括客户端、服务器、网络设备、安全设备等,主机内部资产信息包括硬件资产、操作系统、关键组件及其相关服务、以及各主机开放端口的数量等。网络资产识别技术是一种综合性的网络扫描技术,它综合了操作系统类型扫描和应用端口的深度扫描,相较于NMAP的操作系统指纹识别,网络资产识别技术是在操作系统类型识别的基础上侧重于网络资产的类型识别。各种网络监测工具对主机的端口进行了监控。资产扫描工具(资产识别技术)对网络内各种资产情况进行收集,对资产类型也要分级(例如PC、服务器、网络设备、安全设备等)进行资产价值权重配置。

[0055] 另一方面,利用漏洞扫描技术及工具探测网络漏洞,形成并定期更新漏洞数据库。漏洞数据库不限于本地网络系统采集的内容,也包括在互联网中采集的漏洞数据。漏洞信息及其属性包括网络安全漏洞的数目及等级,各漏洞对应的服务种类及其版本,各漏洞对应的操作系统类型及其版本等。

[0056] 3.利用资产数据库和漏洞数据库进行威胁关联分析

[0057] 上述威胁关联分析包括如下具体内容:

[0058] 1)通过网络安全事件的目的IP,在资产数据库中查找与该IP地址匹配的主机,并且网络安全事件的目的端口在主机上也为已开放状态时,该主机就被网络安全事件命中。

[0059] 2)在资产数据库中,查找主机所拥有的资源情况。这些资源包括硬件、操作系统(OS)、软件和服务、网络带宽使用量等。

[0060] 3)在漏洞数据库中,每个漏洞包含可能受到影响的组件(包括硬件、操作系统、软件和服务等),当这些组件包含在网络安全事件命中的主机中时,这些组件的漏洞就可能被攻击和利用,从而造成可量化的危害和影响。需要对各指标进行赋值,一般的取值都需要经过转化,比如漏洞个数等需要从漏洞扫描报告中提取;攻击次数等指标的提取必须有一个检测模型做数据预处理,再统计得出数值;异常行为分析等也需要建立一个检测模型,用于实时检测;定性数据可通过专家打分的方式转化为定量数据。

[0061] 在进行威胁关联分析时,在基本关联规则的基础上,建立和加载增强关联规则库,对威胁评估结果进行修正和补充。在本发明的一个实施例中,基于大量的现有攻击案例、资产数据库和漏洞数据库,通过对漏洞的分析来追踪和溯源,形成增强关联规则库。

[0062] 如图2所示,当前网络环境下大部分的黑客攻击都是以主机(包括普通PC、服务器、网络设备、安全设备等)为主要攻击对象的,即包括如下步骤:①将目的IP与主机匹配;②攻击找到可利用的漏洞;③如果有组件包含在该漏洞的对象内;④黑客攻击事件命中目标。

[0063] 针对上述的黑客攻击,如图3所示,首先定期刷新资产数据库并定期更新漏洞数据库,然后查询是否有组件包含在该漏洞的对象中?如果是的话,确定发现风险及目标。通过

上述的方式定期进行安全巡查，可以发现风险并产生预警。进一步地，可以用网络安全事件数据、漏洞扫描数据、网络组成资产数据为数据源，然后评估单次供给可能造成的威胁的均值，以及用统一的标准评估这些威胁，为后续的量化分析打下坚实的基础。

[0064] 4.对各个网络安全事件危害指数进行量化评估

[0065] 网络安全事件造成的危害可通过该事件的成本指数来量化，危害程度评估可根据组件级别配置成本及该类网络安全事件造成危害和影响的权重。这个指数可以命名为网络安全事件危害指数，指数越大，表明受威胁程度越高。对该主机造成的危害指数可以由主机所有组件的造成危害指数进行汇总，同样一个网络安全事件对该网络系统造成的危害程度由该网络系统所有主机的造成危害指数来统计汇总。

[0066] 另一方面，网络安全事件危害指数可分为直接损失和间接损失，都可以根据以下公式来量化评估，计算网络安全事件危害指数：

[0067] 网络安全事件危害指数＝成本*权重*命中，即：

[0068] $Host = \sum H_i * Q_i * M_i + \sum Q_j * Q_j * M_j + \sum R_k * Q_k * M_k + \sum S_l * Q_l * M_l$

[0069] $Sys = \sum Host_m$

[0070] 上式中，$Host_m$代表网络安全事件对某个主机造成的危害指数；Sys代表在本监测系统内网络安全事件的危害指数；H_i代表某硬件的成本指数，O_j代表某操作系统的成本指数，R_k代表某组件的成本指数，S_l代表某服务的成本指数，Q代表该类网络安全事件造成危害和影响的权重，M代表网络安全事件是否命中目标。

[0071] 下面进一步说明该公式的编制思路。网络安全事件危害指数衡量安全事件对系统的造成的损失和危害程度，以网络安全事件为主线，通过安全事件关联和事件聚类形成安全威胁的完整攻击链。网络安全事件危害指数由各种安全态势指标根据事件与资产关联、事件与脆弱性关联、事件与事件关联而分析得到，是将事件的损失和危害程度进行综合量化评估后得到的数值，以各安全事件的评估分值加权作为网络安全事件危害指数。网络安全事件危害指数是采集一定时间范围内网络中发生的各种原始安全事件对网络系统内的各种资源造成的损失和危害程度是比较合适和恰当的，它反映了网络安全事件对网络的损失和危害程度，数值越大，代表网络受到的损失和危害程度就越大。

[0072] 其中，成本指数(包括硬件、组件和服务的成本)是通过评估人员手工配置存入数据库，判断主机资产价值的过程就是资产识别的过程，主要从主机内的信息遭到破坏后造成的保密性损失、完整性损失和可用性损失三方面来考虑，根据资产的特点，把资产的价值可以分成高、中和低三个等级。

[0073] M代表网络安全事件是否命中目标，通过图2所示的威胁关联分析中可以得知(安全事件)攻击在与资产、和漏洞的关联中是否命中目标，如果命中M就为1，表示会产生危害，否则M为0，攻击不会产生实际危害。

[0074] Q代表网络安全指标权重，反映了各指标对于网络安全重要性程度，指标权重的来源不同可以分为主观赋权法、客观赋权法和组合赋权法三类。主观赋权法是指人们对分析对象的各个因素，按其重要程度，依照经验，主观确定的权重系数，各个指标权重系数的准确性有赖于专家的知识和经验的积累，客观性较差。客观赋权法主要针对定量指标的权重确定，通过对定量指标实际发生的情况进行统计和整理，从而得出的权重系数，包括熵值法、标准离差法等。这类方法的来源完全客观，但计算方法大多比较繁琐，不利于推广应用。

组合赋权法是结合主观赋权法和客观赋权法的各自优点。首先，在主观赋权法和客观赋权法基础上求出合理的主、客观权重系数，然后根据运用的实际情况确定主、客观权重系数的比例，最后求出综合权重系数。这种方法在一定程度上既反映了决策者的主观信息，又可以利用原始数据和数据模型，使权重系数具有客观性。但是其准确性有赖于对主、客观赋权法权重系数所占比例的确定。在实际运用过程中，主观赋权法因其简便性而应用最为广泛。评价指标权重确定对于网络安全评价是至关重要的。

[0075] 上述网络安全事件危害指数评估方法通过对网络系统内发生安全事件进行分析，根据安全事件与资产、漏洞等对应关系及时发现正在发生的安全相关活动和事件，并分析这些活动的危害程度和严重级别，评估和量化网络安全事件造成的危害(或影响)指数，对安全威胁做出直接的反馈，让最有效的策略最快提出，确保整个系统的安全。当攻击者发起攻击时，能够在最短的时间内发现和预警，便于准备应急和处置方案。

[0076] 在上述网络安全事件危害指数评估方法的基础上，本发明进一步提供了一种采用该方法的网络安全态势感知系统。如图4所示，该网络安全态势感知系统包括位于核心区的安全响应与策略配置单元、安全关联分析单元、安全事件统计分析单元、网络安全事件危害指数量化单元和安全态势评估单元。其中，以网络安全事件危害指数量化单元为中心。该单元分别从安全响应与策略配置单元、安全关联分析单元、安全事件统计分析单元中获取数据，以执行上述的网络安全事件危害指数评估方法。另外，网络安全事件危害指数量化单元与安全态势评估单元之间交互数据，针对特定的威胁给网络系统带来的威胁进行量化，为后续深入评估和预测提供参考。

[0077] 除了上述各功能单元之外，该网络安全态势感知系统还包括安全数据采集单元、数据库、知识库以及管理支撑子系统。其中，安全数据采集单元分别向安全响应与策略配置单元、安全关联分析单元、安全事件统计分析单元提供所采集的基础安全数据，数据库、知识库以及管理支撑子系统与位于核心区的各个功能单元连接，向它们提供基础的数据支撑服务。

[0078] 下面，结合图5进一步说明该网络安全态势感知系统如何应用本发明所提供的网络安全事件危害指数评估方法。

[0079] 步骤1:安全态势数据采集

[0080] 数据采集为网络安全态势感知提出基础数据源，是态势评估过程的第一步。在本发明的一个实施例中，可以采用SnMp和Syslog收集网络流量信息、日志信息等，通过配置不同的网络安全设备，完成对各类安全态势数据的采集。

[0081] 步骤2:数据预处理及其安全事件鉴别

[0082] 网络数据具有不确定性、不完整性、变异性和模糊性的特点，为了对其进行更好的分析和处理，就需要对其进行数据预处理。并对其类似的进行合并，减少重复报警概率；从多个层面，多个维度，对网络安全设备所报告的安全事件进行进一步分析与可信度验证，减少告警冗余，发现综合安全事件，并根据这些信息生成安全事件的分析模型，用于对安全事件的自动鉴别

[0083] 步骤3:威胁关联分析

[0084] 为得到有用的信息，首先应对原始报警数据进行去重与合并，然后进行关联分析。事件关联是指找出大量事件中存在的关系，并从这些大量事件中抽取出真正重要的少量事

件。借助先进的智能事件关联分析引擎，系统能够实时不间断地对所有范式化后的日志流进行安全事件关联分析。

[0085] 步骤4：指标定义及其危害指数评定

[0086] 为了定量描述网络态势，需要定量描述各个网络性质的指标数据用来形成网络安全指数，从不同视角对网络的安全态势进行定量描述。构建合理的安全态势指标体系是对网络安全态势进行合理评估和预测的必要条件。为此，可以采用图1所示的网络安全事件危害指数评估方法对网络状态进行分析处理，以便发现真正的网络风险点，提高评估和预测的准确性。

[0087] 步骤5：指标合成及安全总体指数综合评价

[0088] 根据单因素模糊综合评判法，对各叶节点指标按照分类进行10分制的评价，分值反映了叶节点的安全指标的指数。由上一步单因素评估得出的结果数据进行下一级模糊综合评价，得出评价结果，包括综合评价得分以及相应的网络安全等级。

[0089] 从网络安全性出发并确保态势感知结果能够指导管理实践，我们建立了如图6所示的网络安全态势综合感知体系，将安全量化指标共分为三级。网络安全态势综合感知体系的建立是从上层网络安全管理的需求出发层层分解而得的，上一级安全指标指数由下一级安全指标关联分析和综合评估得到，最下层的指标还需要和能采集到的数据相关联以保证指标数值的真实性和准确性。

[0090] 一级指标即网络安全事件危害指数，网络安全事件危害指数是采集一定时间范围内网络中发生的各种原始安全事件造成的损失和危害程度，由所有单个网络安全事件危害指数的总和来确定。为了定量描述网络安全事件危害指数，需定义了定量描述各个网络性质的指标数据，分别为基础运行指数、脆弱性指数和威胁指数这三个二级指标，用来量化各网络安全事件危害指数。

[0091] 二级指标由基础设施运行安全指数、脆弱性指数和威胁指数组成。

[0092] 基础设施运行安全指数是采集一定时间范围内的各资产的网络运行的数据，进行量化评估后得到的数值，它反映网络当前的运行状态，数值越大，代表网络运行状态越差。

[0093] 脆弱性指数是通过量化漏洞数目等信息和系统安全防护软件安装配置情况来综合生成脆弱性指数，可以从整体上来衡量网络面临威胁时可能损失的程度。它关注当前网络在遭受攻击情况下，能够承受的攻击的严重程度。数值越大，代表网络越容易遭受攻击，损失越大。

[0094] 威胁指数是采集一定时间范围内网络中发生的各种原始安全事件，把事件的属性值进行综合量化评估后得到的数值，它反映了网络安全事件对网络的威胁程度，数值越大，代表网络受到的威胁程度越大。

[0095] 二级指标由其对应的三级指标组成，三级指标较多，不一一叙述。如基础设施运行安全指数由(主机/服务器)资产价值、操作系统信息、关键服务组件及服务等三级指标组成。

[0096] 步骤6：进行整体网络安全态势的评估

[0097] 整体网络安全态势由安全态势综合指数来衡量。安全态势综合指数在一定时间窗口内综合考虑影响网络安全态势的各种因素，采用一定的方法进行综合量化评估后得到的一个反映网络整体安全态势的向量，安全态势综合安全指数由所有单个网络安全事件危害

指数的总和来确定。根据以上指数评估方法并结合安全态势的危险性、可靠性、脆弱性、可用性等评价向量进行矩阵相乘形成综合评价向量，根据综合评价向量和评价标准进行整体网络安全态势的评估。

[0098] 步骤7：展示安全态势

[0099] 根据网络安全态势评估的结果，展示系统安全态势评估结果及网络拓扑结构图中不同网络节点的网络安全状况信息，以及不同指标下的网络安全态势信息以及网络安全告警信息查询等，从而给管理人员提供决策支持。

[0100] 与现有技术相比较，本发明是建立在资产数据库和漏洞数据库基础上的网络安全态势量化评估方法，利用威胁建模测算出攻击事件对安全网络造成的危害，然后针对特定的威胁攻击给安全系统带来的威胁进行量化，考虑影响网络安全的因素包括安全事件、主机漏洞以及提供的服务等，并根据安全活动与资产、漏洞等对应关系，分析这些活动的危害程度，评估的结果更加准确和可信。

[0101] 上面对本发明所提供的基于多维关联的网络安全事件危害指数评估方法及其系统进行了详细的说明。对本领域的一般技术人员而言，在不背离本发明实质精神的前提下对它所做的任何显而易见的改动，都将构成对本发明专利权的侵犯，将承担相应的法律责任。

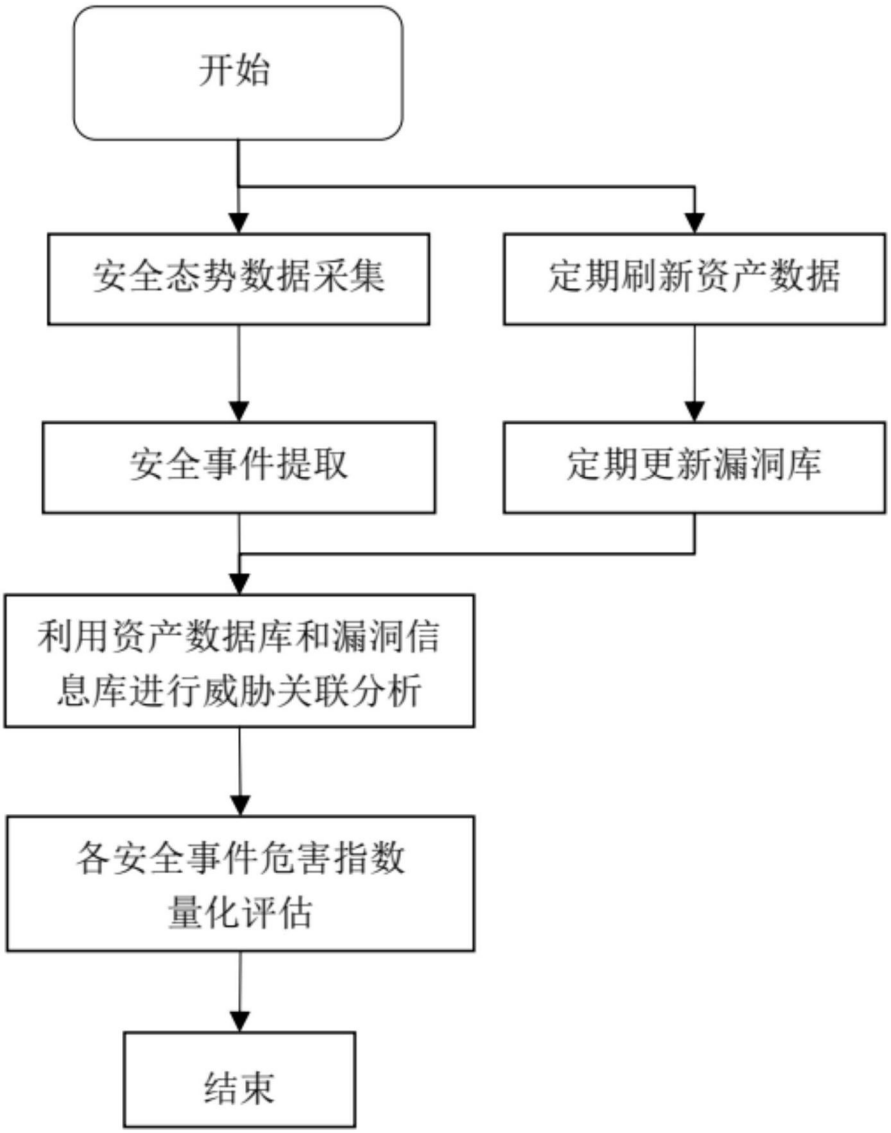

开始
安全态势数据采集
定期刷新资产数据
安全事件提取
定期更新漏洞库
利用资产数据库和漏洞信息库进行威胁关联分析
各安全事件危害指数量化评估
结束

图1

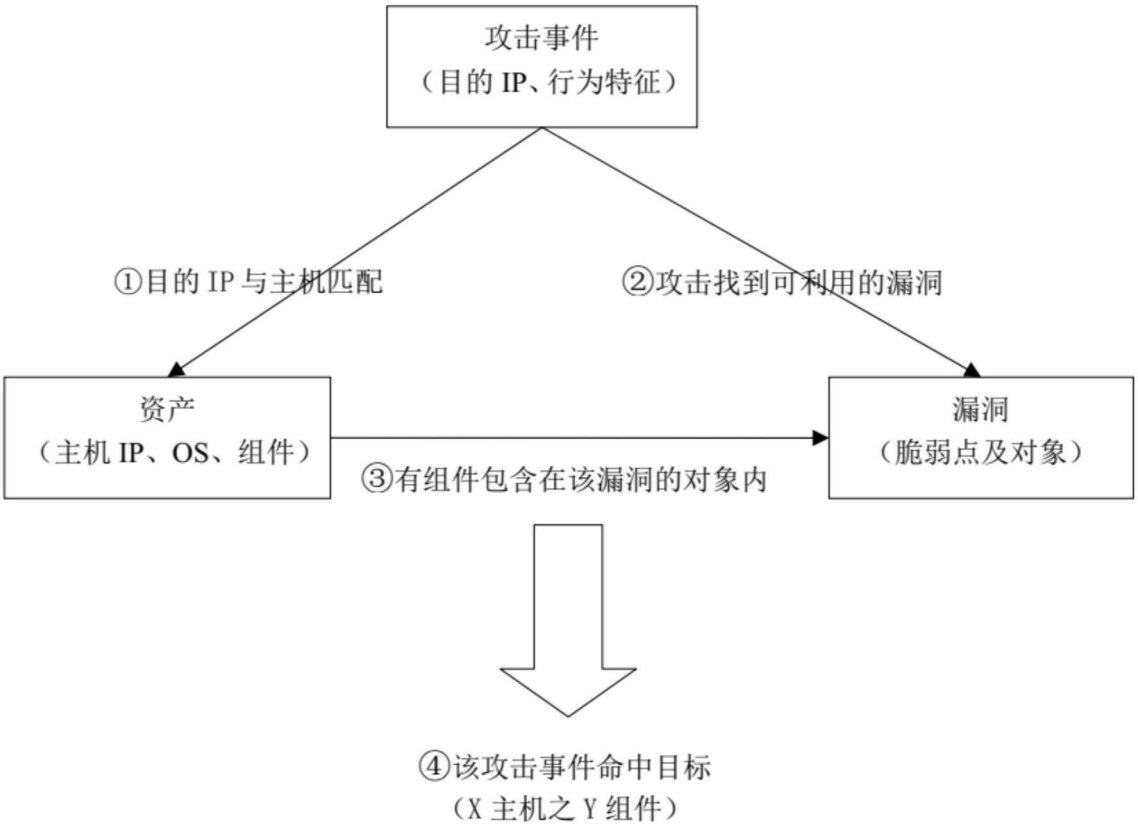

攻击事件
（目的 IP、行为特征）
①目的 IP 与主机匹配
②攻击找到可利用的漏洞
资产
（主机 IP、OS、组件）
漏洞
（脆弱点及对象）
③有组件包含在该漏洞的对象内
④该攻击事件命中目标
（X 主机之 Y 组件）

图2

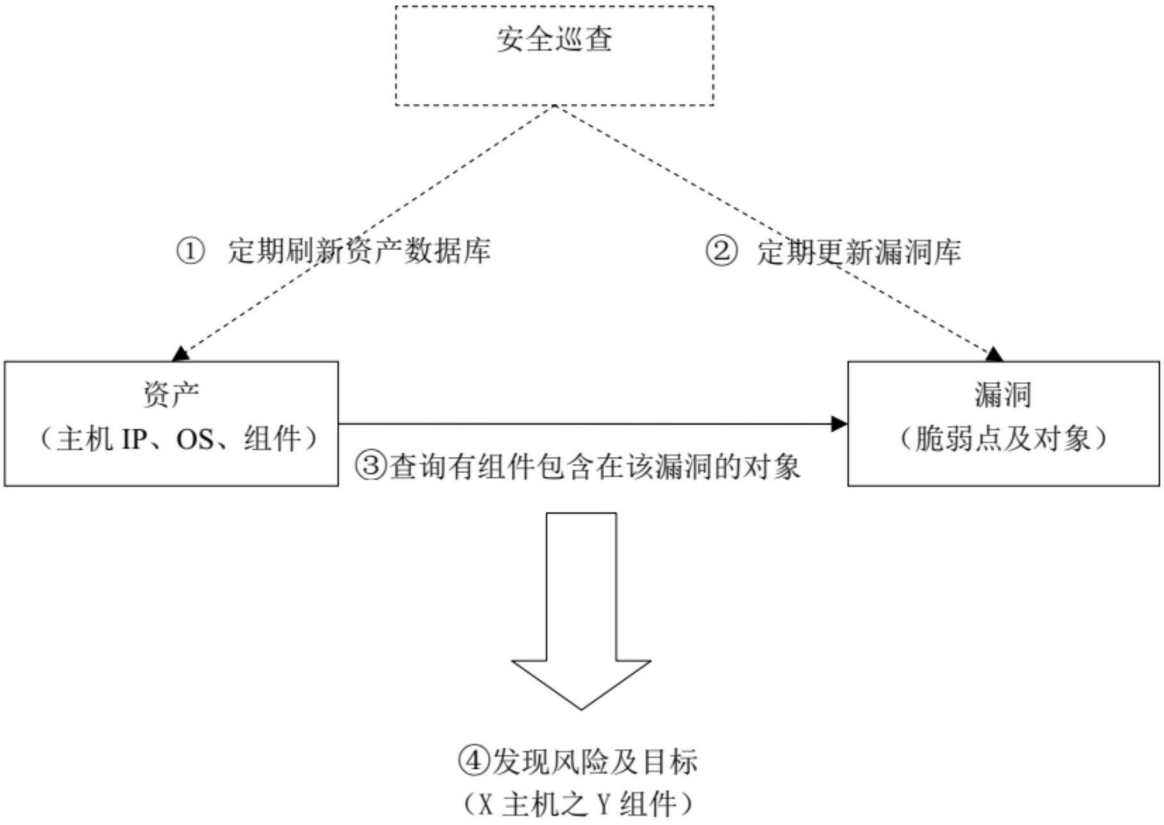

安全巡查
① 定期刷新资产数据库
② 定期更新漏洞库
资产
（主机 IP、OS、组件）
漏洞
（脆弱点及对象）
③查询有组件包含在该漏洞的对象
④发现风险及目标
（X 主机之 Y 组件）

图3

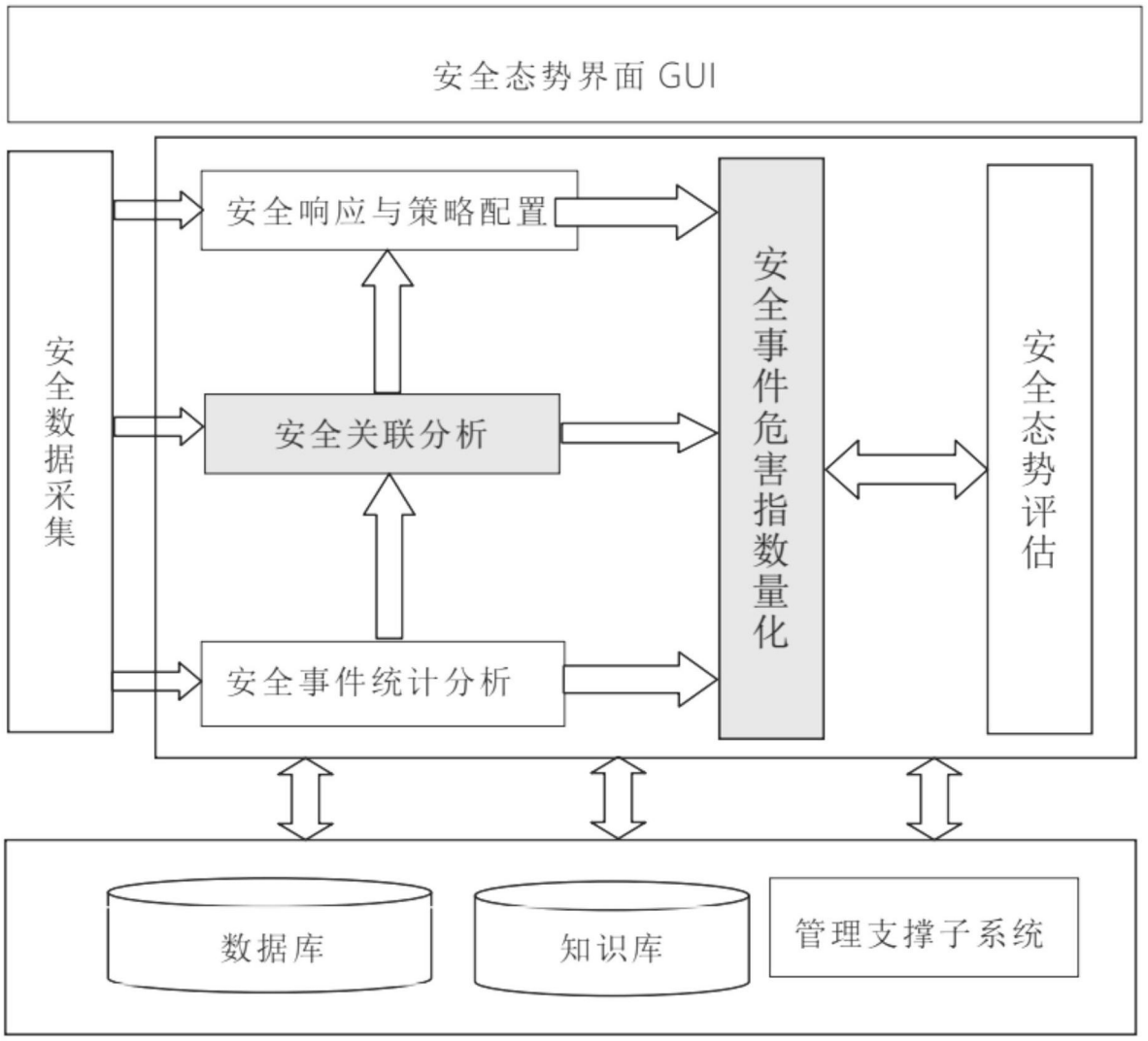

安全态势界面 GUI
安全数据采集
安全响应与策略配置
安全关联分析
安全事件统计分析
安全事件危害指数量化
安全态势评估
数据库
知识库
管理支撑子系统

图4

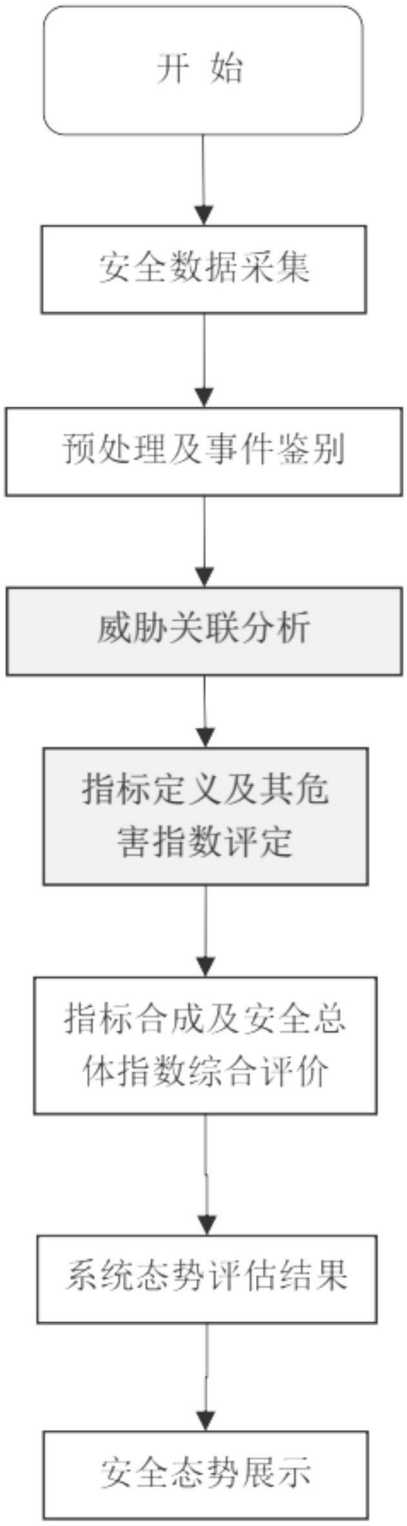

开 始
安全数据采集
预处理及事件鉴别
威胁关联分析
指标定义及其危害指数评定
指标合成及安全总体指数综合评价
系统态势评估结果
安全态势展示

图5

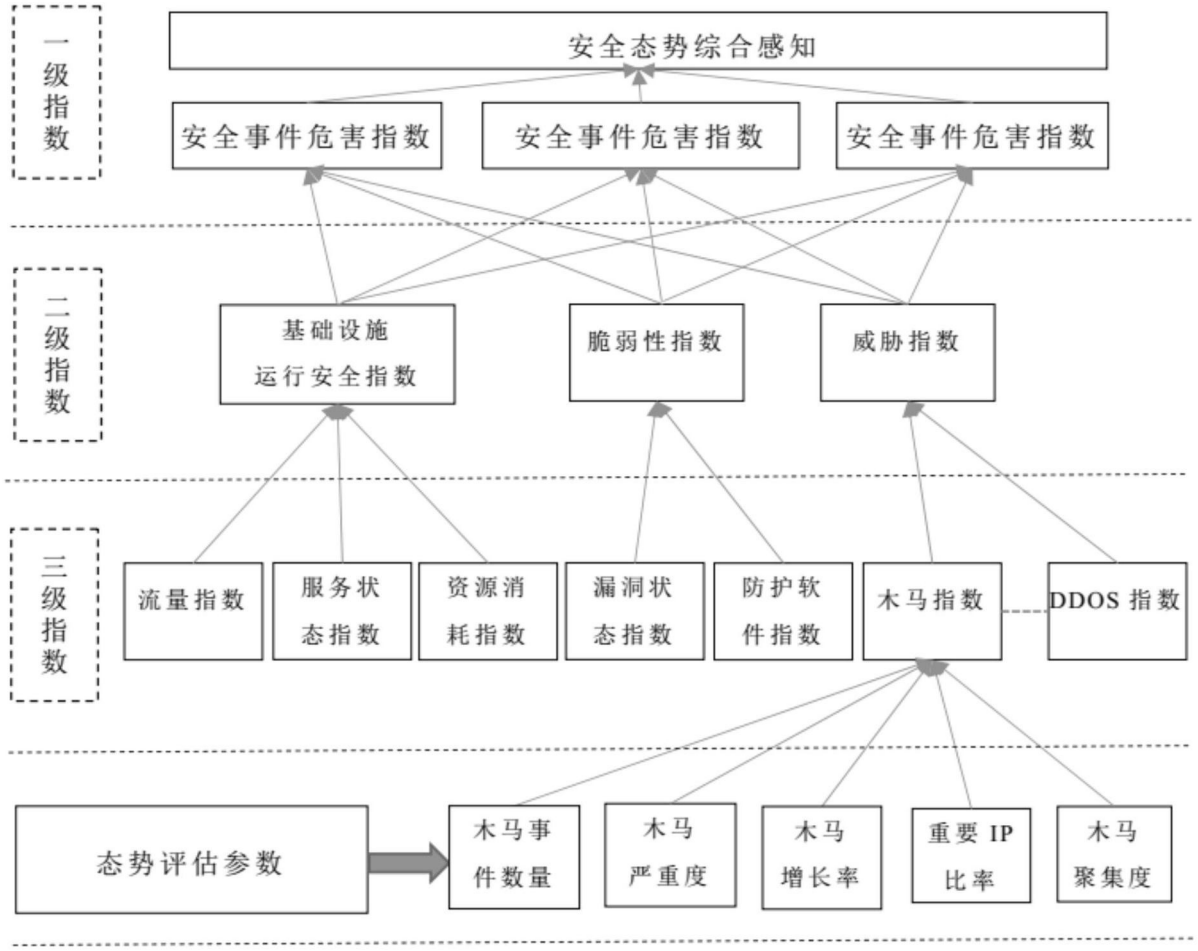

一级指数
安全态势综合感知
安全事件危害指数
安全事件危害指数
安全事件危害指数
二级指数
基础设施运行安全指数
脆弱性指数
威胁指数
三级指数
流量指数
服务状态指数
资源消耗指数
漏洞状态指数
防护软件指数
木马指数
DDOS 指数
态势评估参数
木马事件数量
木马严重度
木马增长率
重要 IP 比率
木马聚集度

图6