(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116800536 A
(43)申请公布日 2023.09.22

(21)申请号 202310944878.X

(22)申请日 2023.07.28

(71)申请人 吴锦豪
地址 201210 上海市浦东新区张江镇环东村三灶路1380弄12号

(72)发明人 吴锦豪

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

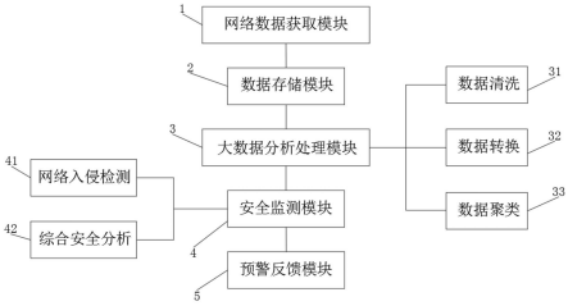
权利要求书2页 说明书4页 附图1页

(54)发明名称

一种基于大数据分析的网络安全监测系统

(57)摘要

本发明公开了一种基于大数据分析的网络安全监测系统，涉及网络安全监测技术领域，包括网络数据获取模块、数据存储模块、大数据分析处理模块、安全监测模块和预警反馈模块。本发明通过大数据分析处理模块对海量网络数据的数据清洗、数据转换和数据聚类处理，提高网络安全监测的精度和适配性，并通过对网络入侵行为的检测和安全分析，使得本系统能够预测网络安全风险并对入侵行为进行溯源分析，在网络异常行为发生时快速发现，与监控终端进行行为信息反馈，进而实现快速应急响应，通过利用网络数据获取模块对网络中各节点信息进行采集处理，提高网络监测的范围。



CN 116800536 A

1.一种基于大数据分析的网络安全监测系统，其特征在于：包括网络数据获取模块(1)、数据存储模块(2)、大数据分析处理模块(3)、安全监测模块(4)和预警反馈模块(5)；

所述网络数据获取模块(1)用于获取网络各个节点位置数据并设置采集持续时间和采集间隔，实现对系统网络数据的实时采集；

所述数据存储模块(2)用于将采集数据进行分类处理并构建数据库为采集数据提供存储空间，将数据进行存储备份；

所述大数据分析处理模块(3)用于根据采集的网络数据利用大数据技术进行分析处理，包括数据清洗(31)、数据转换(32)和数据聚类(33)；

所述安全监测模块(4)用于对网络数据进行安全监测，综合分析发现潜在的攻击威胁并发布预警信息，包括网络入侵检测(41)和综合安全分析(42)；

所述预警反馈模块(5)用于与监控终端进行实时信息交互，在接收预警信息后快速向监控终端反馈进行应急响应。

2.根据权利要求1所述的一种基于大数据分析的网络安全监测系统，其特征在于：所述网络数据获取模块(1)采集数据包括网络流量采集、日志采集和资产和漏洞数据采集。

3.根据权利要求2所述的一种基于大数据分析的网络安全监测系统，其特征在于：所述网络流量采集用于在互联网出入口、云边界等重要网络出入口采集原始流量数据，使用探针旁路部署模式，与路由器、交换机或防火墙等网络安全设备镜像端口相连，不改变原有的网络结构，获得链路中流量数据的拷贝。

4.根据权利要求2所述的一种基于大数据分析的网络安全监测系统，其特征在于：所述日志采集利用Flume组件采集网络中的各类型数据，将数据格式化封装到事件里，写入数据传输通道，实现日志采集、过滤、缓存、中转分发和调度。

5.根据权利要求2所述的一种基于大数据分析的网络安全监测系统，其特征在于：所述资产和漏洞数据采集中，网络资产包括终端、服务器、网络安全设备、物联网设备等，漏洞数据采集分为主动扫描和被动扫描，主动扫描识别资产中的漏洞、配置、弱密码、Web明文传输等风险，被动扫描是在分析用户主机遭受攻击后，识别出用户主机的安全漏洞风险。

6.根据权利要求1所述的一种基于大数据分析的网络安全监测系统，其特征在于：所述数据清洗(31)用于对网络数据进行过滤处理和缺失数据补充，采用门限补偿的处理方式，所述数据转换(32)包括单位换算、数据泛化和规范化，其中数据规范化包括归一化处理和标准化处理，所述数据聚类(33)基于数据转换(32)结果进行聚类处理。

7.根据权利要求1所述的一种基于大数据分析的网络安全监测系统，其特征在于：所述网络入侵检测(41)用于提取入侵行为特征码，将其归结为协议中不同领域的特征值，编写相应的检测规则，通过将预处理的数据包与规则库中的每个规则匹配，检测到由特征值决定的入侵行为是否发生。

8.根据权利要求1所述的一种基于大数据分析的网络安全监测系统，其特征在于：所述综合安全分析(42)包括异常流量分析、异常行为分析、恶意代码分析和攻击威胁溯源。

9.根据权利要求8所述的一种基于大数据分析的网络安全监测系统，其特征在于：所述异常流量分析用于提取原始流量日志，基于机器学习、关联分析引擎对未知异常流量检测和未知攻击事件的分析发现；

所述异常行为分析利用UEBA分析技术，结合威胁情报库和主机访问异常等各种异常行

为事件，以聚类方式识别和划分具有相似行为、属性的群体，通过群体分析发现异常行为，预测未知风险。

10.根据权利要求8所述的一种基于大数据分析的网络安全监测系统，其特征在于：所述恶意代码分析用于监测捕获多种来源恶意代码，分析样本行为和同源性，获得恶意代码的演进过程、行为特征、事件关联等主要数据，建立入库恶意代码样本和数据的索引查询；

所述攻击威胁溯源从网络流量、日志数据、威胁情报、恶意样本等多维度，关联分析攻击者的入侵方式，还原攻击事件的整个过程，实现安全溯源分析。

一种基于大数据分析的网络安全监测系统

技术领域

[0001] 本发明涉及网络安全监测技术领域，具体为一种基于大数据分析的网络安全监测系统。

背景技术

[0002] 互联网的飞速发展为人类的生产生活带来了极大的便利，同时也对当前的互联网安全形成了一定的挑战，并暴露出了由于网络安全技术漏洞、安全漏洞等诸多因素引起的网络安全问题。

[0003] 如中国专利号为:CN115987695A的“一种基于大数据分析的网络安全监测系统”，包括数据接收模块、数据分类模块、安全监测模块、分布式数据库和数据备份模块;数据接收模块用于对不同IP所上传或编辑的网络信息、网络数据和网络内容进行收集，得到IP编辑数据;云端服务器接收到IP编辑数据后，利用数据分类模块对缓存的IP编辑数据进行监测系数分析，生成IP编辑数据的监测优先表;提高数据监测效率;安全监测模块用于判断IP编辑数据是否存在网络危险;数据备份模块用于对不存在危险的IP编辑数据进行备份;并选取空余系数最大的存储区块作为选中区块。

[0004] 但现有技术中，目前网络安全监测对海量网络数据的分析处理能力较弱，在网络监测过程中存在监测范围小、监测精度低的问题，对于网络中异常行为不易快速发现并进行及时预警响应。

发明内容

[0005] 本发明的目的在于提供一种基于大数据分析的网络安全监测系统，以解决上述背景技术提出的目前网络安全监测对海量网络数据的分析处理能力较弱，在网络监测过程中存在监测范围小、监测精度低的问题，对于网络中异常行为不易快速发现并进行及时预警响应的问题。

[0006] 为实现上述目的，本发明提供如下技术方案:一种基于大数据分析的网络安全监测系统，包括网络数据获取模块、数据存储模块、大数据分析处理模块、安全监测模块和预警反馈模块;

[0007] 所述网络数据获取模块用于获取网络各个节点位置数据并设置采集持续时间和采集间隔，实现对系统网络数据的实时采集;

[0008] 所述数据存储模块用于将采集数据进行分类处理并构建数据库为采集数据提供存储空间，将数据进行存储备份;

[0009] 所述大数据分析处理模块用于根据采集的网络数据利用大数据技术进行分析处理，包括数据清洗、数据转换和数据聚类;

[0010] 所述安全监测模块用于对网络数据进行安全监测，综合分析发现潜在的攻击威胁并发布预警信息，包括网络入侵检测和综合安全分析;

[0011] 所述预警反馈模块用于与监控终端进行实时信息交互，在接收预警信息后快速向

监控终端反馈进行应急响应。

[0012] 优选的，所述网络数据获取模块采集数据包括网络流量采集、日志采集和资产和漏洞数据采集。

[0013] 优选的，所述网络流量采集用于在互联网出入口、云边界等重要网络出入口采集原始流量数据，使用探针旁路部署模式，与路由器、交换机或防火墙等网络安全设备镜像端口相连，不改变原有的网络结构，获得链路中流量数据的拷贝，主要用于监听和检测网络中的数据流及各类异常行为。

[0014] 优选的，所述日志采集利用Flume组件采集网络中的各类型数据，将数据格式化封装到事件里，写入数据传输通道，实现日志采集、过滤、缓存、中转分发和调度。

[0015] 优选的，所述资产和漏洞数据采集中，网络资产包括终端、服务器、网络安全设备、物联网设备等，漏洞数据采集分为主动扫描和被动扫描，主动扫描识别资产中的漏洞、配置、弱密码、Web明文传输等风险，被动扫描是在分析用户主机遭受攻击后，识别出用户主机的安全漏洞风险。

[0016] 优选的，所述数据清洗用于对网络数据进行过滤处理和缺失数据补充，采用门限补偿的处理方式，所述数据转换包括单位换算、数据泛化和规范化，其中数据规范化包括归一化处理和标准化处理，所述数据聚类基于数据转换结果进行聚类处理。

[0017] 优选的，所述网络入侵检测用于提取入侵行为特征码，将其归结为协议中不同领域的特征值，编写相应的检测规则，通过将预处理的数据包与规则库中的每个规则匹配，检测到由特征值决定的入侵行为是否发生。

[0018] 优选的，所述综合安全分析包括异常流量分析、异常行为分析、恶意代码分析和攻击威胁溯源。

[0019] 优选的，所述异常流量分析用于提取原始流量日志，基于机器学习、关联分析引擎对未知异常流量检测和未知攻击事件的分析发现；所述异常行为分析利用UEBA分析技术，结合威胁情报库和主机访问异常等各种异常行为事件，以聚类方式识别和划分具有相似行为、属性的群体，通过群体分析发现异常行为，预测未知风险。

[0020] 优选的，所述恶意代码分析用于监测捕获多种来源恶意代码，分析样本行为和同源性，获得恶意代码的演进过程、行为特征、事件关联等主要数据，建立入库恶意代码样本和数据的索引查询；所述攻击威胁溯源从网络流量、日志数据、威胁情报、恶意样本等多维度，关联分析攻击者的入侵方式，还原攻击事件的整个过程，实现安全溯源分析。

[0021] 与现有技术相比，本发明的有益效果是：

[0022] 本发明中，通过大数据分析处理模块对海量网络数据的数据清洗、数据转换和数据聚类处理，提高网络安全监测的精度和适配性，并通过对网络入侵行为的检测和安全分析，使得本系统能够预测网络安全风险并对入侵行为进行溯源分析，在网络异常行为发生时快速发现，与监控终端进行行为信息反馈，进而实现快速应急响应，通过利用网络数据获取模块对网络中各节点信息进行采集处理，提高网络监测的范围。

附图说明

[0023] 图1为本发明一种基于大数据分析的网络安全监测系统的系统框图。

[0024] 图中：1、网络数据获取模块；2、数据存储模块；3、大数据分析处理模块；31、数据清

洗;32、数据转换;33、数据聚类;4、安全监测模块;41、网络入侵检测;42、综合安全分析;5、预警反馈模块。

具体实施方式

[0025] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整的描述,显然,所描述的实施条例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0026] 参照图1所示:一种基于大数据分析的网络安全监测系统,包括网络数据获取模块1、数据存储模块2、大数据分析处理模块3、安全监测模块4和预警反馈模块5;

[0027] 其中,网络数据获取模块1用于获取网络各个节点位置数据并设置采集持续时间和采集间隔,实现对系统网络数据的实时采集;具体的,网络数据获取模块1采集数据包括网络流量采集、日志采集和资产和漏洞数据采集,网络流量采集用于在互联网出入口、云边界等重要网络出入口采集原始流量数据,使用探针旁路部署模式,与路由器、交换机或防火墙等网络安全设备镜像端口相连,不改变原有的网络结构,获得链路中流量数据的拷贝,主要用于监听和检测网络中的数据流及各类异常行为,日志采集利用Flume组件采集网络中的各类型数据,将数据格式化封装到事件里,写入数据传输通道,实现日志采集、过滤、缓存、中转分发和调度,资产和漏洞数据采集中,网络资产包括终端、服务器、网络安全设备、物联网设备等,漏洞数据采集分为主动扫描和被动扫描,主动扫描识别资产中的漏洞、配置、弱密码、Web明文传输等风险,被动扫描是在分析用户主机遭受攻击后,识别出用户主机的安全漏洞风险,按照漏洞扫描结果、资产重要性及漏洞的威胁情报,排序漏洞重要性,以确定修复的优先级,通过利用网络数据获取模块1对网络中各节点信息进行采集处理,提高网络监测的范围。

[0028] 其中,数据存储模块2用于将采集数据进行分类处理并构建数据库为采集数据提供存储空间,将数据进行存储备份,选择MySQL作为网络安全监测系统数据库的运行环境,通过对监控网络中各个节点的位置和运行数据的收集与存储,利用数据存储模块2将采集数据进行存储,实现网络数据随时间变化逐渐增加进行实时备份,便于后续数据分析处理进行数据的调取。

[0029] 其中,大数据分析处理模块3用于根据采集的网络数据利用大数据技术进行分析处理,包括数据清洗31、数据转换32和数据聚类33;具体的,数据清洗31用于对网络数据进行过滤处理和缺失数据补充,采用门限补偿的处理方式,数据转换32包括单位换算、数据泛化和规范化,其中数据规范化包括归一化处理和标准化处理,数据聚类33基于数据转换32结果进行聚类处理,方便进行网络数据特征的提取与分析,便于后续网络异常行为的分析处理。

[0030] 其中,安全监测模块4用于对网络数据进行安全监测,综合分析发现潜在的攻击威胁并发布预警信息,包括网络入侵检测41和综合安全分析42;具体的,网络入侵检测41用于提取入侵行为特征码,将其归结为协议中不同领域的特征值,编写相应的检测规则,通过将预处理的数据包与规则库中的每个规则匹配,检测到由特征值决定的入侵行为是否发生,综合安全分析42包括异常流量分析、异常行为分析、恶意代码分析和攻击威胁溯源,异常流

量分析用于提取原始流量日志，基于机器学习、关联分析引擎对未知异常流量检测和未知攻击事件的分析发现；异常行为分析利用UEBA分析技术，结合威胁情报库和主机访问异常等各种异常行为事件，以聚类方式识别和划分具有相似行为、属性的群体，通过群体分析发现异常行为，预测未知风险；恶意代码分析用于监测捕获多种来源恶意代码，分析样本行为和同源性，获得恶意代码的演进过程、行为特征、事件关联等主要数据，建立入库恶意代码样本和数据的索引查询；攻击威胁溯源从网络流量、日志数据、威胁情报、恶意样本等多维度，关联分析攻击者的入侵方式，还原攻击事件的整个过程，实现安全溯源分析。

[0031] 其中，预警反馈模块5用于与监控终端进行实时信息交互，在网络异常行为发生时，在接收预警信息后快速向监控终端进行异常行为信息反馈，进而实现快速应急响应。

[0032] 本发明的工作原理：通过利用网络数据获取模块1对网络中各节点信息进行采集处理，提高网络监测的范围，利用数据存储模块2将采集数据进行存储，实现网络数据随时间变化逐渐增加进行实时备份，便于后续数据分析处理进行数据的调取，通过大数据分析处理模块3对海量网络数据的数据清洗31、数据转换32和数据聚类33处理，提高系统网络安全监测精度和适配性，并配合安全监测模块4对网络入侵行为的检测和安全分析，使得本系统能够预测网络安全风险并对入侵行为进行溯源分析，在网络异常行为发生时快速发现，并通过预警反馈模块5与监控终端进行异常行为信息反馈，进而实现快速应急响应。

[0033] 尽管参照前述实施例对本发明进行了详细的说明，对于本领域的技术人员来说，其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

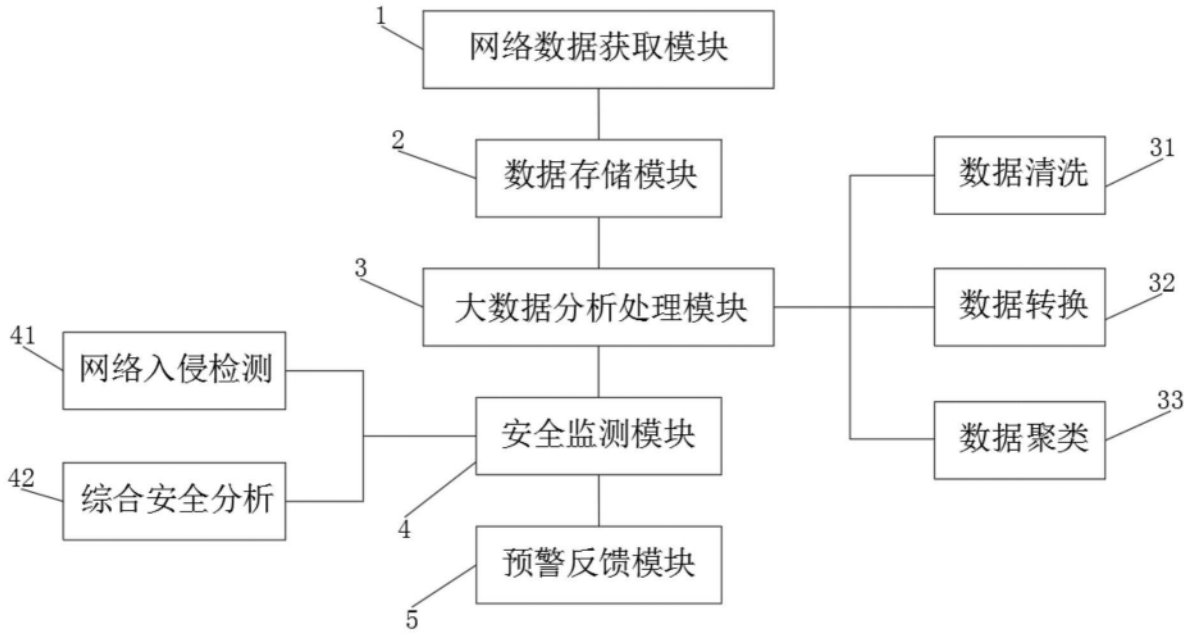

1
网络数据获取模块
2
数据存储模块
3
大数据分析处理模块
31
数据清洗
32
数据转换
33
数据聚类
41
网络入侵检测
42
综合安全分析
安全监测模块
4
预警反馈模块
5

图1