(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 103875222 A
(43)申请公布日 2014.06.18

(21)申请号 201280045112.8
(22)申请日 2012.09.14
(30)优先权数据
13/233497 2011.09.15 US
(85)PCT国际申请进入国家阶段日
2014.03.17
(86)PCT国际申请的申请数据
PCT/US2012/055630 2012.09.14
(87)PCT国际申请的公布数据
WO2013/040496 EN 2013.03.21
(71)申请人 迈可菲公司
地址 美国加利福尼亚州
(72)发明人 Z. 布 R.C. 卡斯亚普 Y. 林
D.L.H. 马
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 杨美灵 汤春龙
(51)Int.Cl.
H04L 29/06(2006.01)

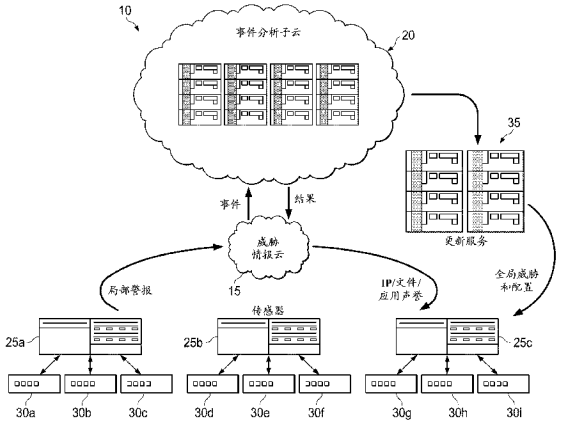
权利要求书2页 说明书6页 附图3页

(54)发明名称

用于实时定制的威胁防护的系统和方法

(57)摘要

在一个示范实施例中提供一种方法，该方法包括：接收与来自遍及网络环境分布的传感器的报告相关联的事件信息以及使事件信息相互关联以识别威胁。基于威胁的定制的安全策略可以被发送到传感器。



CN 103875222 A

1. 一种方法，包括：接收与来自遍及网络环境分布的传感器的报告相关联的事件信息；使所述事件信息相互关联以识别威胁；以及基于所述威胁将定制的安全策略发送到所述传感器中的至少一个。

2. 根据权利要求 1 所述的方法，还包括基于所述威胁将声誉数据发送到声誉系统。

3. 根据权利要求 1 所述的方法，还包括基于所述威胁将声誉数据发送到威胁情报云。

4. 根据权利要求 1 所述的方法，其中所述传感器包括防止入侵系统。

5. 根据权利要求 1 所述的方法，其中所述定制的安全策略隔离感染有所述威胁的主机。

6. 根据权利要求 1 所述的方法，其中所述事件信息是从威胁情报云接收的。

7. 根据权利要求 1 所述的方法，还包括基于新的威胁将声誉数据发送到威胁情报云，以及其中所述事件信息是从威胁情报云接收的，所述传感器包括防止入侵系统，且所述定制的安全策略隔离感染有所述新的威胁的主机。

8. 在一个或更多非短暂性介质中编码的逻辑，所述逻辑包括用于运行的代码且当所述代码由一个或更多处理器运行时所述代码可操作来执行包括以下操作的操作：接收与来自遍及网络环境分布的传感器的报告相关联的事件信息；使所述事件信息相互关联以识别威胁；以及基于所述威胁将定制的安全策略发送到所述传感器中的至少一个。

9. 根据权利要求 8 所述的编码的逻辑，其中所述操作还包括基于所述威胁将声誉数据发送到声誉系统。

10. 根据权利要求 8 所述的编码的逻辑，其中所述操作还包括基于所述威胁将声誉数据发送到威胁情报云。

11. 根据权利要求 8 所述的编码的逻辑，其中所述传感器包括防止入侵系统。

12. 根据权利要求 8 所述的编码的逻辑，其中所述定制的安全策略隔离感染有所述威胁的主机。

13. 根据权利要求 8 所述的编码的逻辑，其中所述事件信息是从威胁情报云接收的。

14. 一种装置，包括：一个或更多处理器，可操作来运行与事件分析子云相关联的指令使得所述装置配置成：接收与来自遍及网络环境分布的传感器的报告相关联的事件信息；使所述事件信息相互关联以识别威胁；以及基于所述威胁将定制的安全策略发送到所述传感器中的至少一个。

15. 根据权利要求 14 所述的装置，其中所述装置还配置成基于所述威胁将声誉数据发送到声誉系统。

16. 根据权利要求 14 所述的装置，其中所述装置还配置成基于所述威胁将声誉数据发送到威胁情报云。

17. 根据权利要求 14 所述的装置，其中所述传感器包括防止入侵系统。

18. 根据权利要求 14 所述的装置，其中所述定制的安全策略隔离感染有所述威胁的主机。

19. 根据权利要求 14 所述的装置，其中所述事件信息是从威胁情报云接收的。

20. 一种装置，包括：威胁情报云；事件分析子云；以及一个或更多处理器，可操作来运行与所述威胁情报云和所述事件分析子云相关联的指令使得：所述威胁情报云配置成接收与来自遍及网络环境分布的传感器的报告相关联的事件信息；以及所述事件分析子云配

置成使所述事件信息相互关联以识别威胁以及基于所述威胁将定制的安全策略发送到所述传感器中的至少一个。

用于实时定制的威胁防护的系统和方法

技术领域

[0001] 本说明书一般涉及网络安全的领域，更具体地涉及用于实时定制的威胁防护的系统和方法。

背景技术

[0002] 信息系统已经在全球规模上逐渐融入人们的日常生活和工作中，且信息安全的领域已经同样地在现在的社会中变得愈加重要。这样大规模的融合还为恶意操作者展现了许多利用这些系统的机会。如果恶意软件能感染主计算机，则它能执行任意数量的恶意行动，如从主计算机发出垃圾邮件或恶意邮件、从与主计算机相关联的企业或个人盗取敏感信息、向其它主计算机传播和 / 或帮助分布式拒绝服务攻击。此外，对于一些类型的恶意软件，恶意操作者能向其它恶意操作者出售或者以其它方式给予访问权，由此扩大对主计算机的利用。因此，有效保护并维持稳定的计算机和系统的能力仍然对于组件制造商、系统设计者和网络运营商提出很大的挑战。

附图说明

[0003] 为了提供对本公开及其特点和优点的更全面的理解，参照结合附图进行的以下描述，其中相似的附图标记表示相似的部分，其中 ：

图 1 是示出根据本说明书的用于实时定制的威胁防护的网络环境的示范实施例的简化框图 ；以及

图 2 是可与该网络环境相关联的潜在操作的简化交互图。

[0004] 图 3 是可与该网络环境相关联的潜在操作的简化流程图。

具体实施方式

[0005] 概述

在一个示范实施例中提供一种方法，该方法包括 ：接收与来自遍及网络环境分布的传感器的报告相关联的事件信息以及使事件信息相互关联以识别威胁。基于威胁的定制的安全策略可以被发送到传感器。在更具体的实施例中，可从威胁情报云接收事件信息。在另外的实施例中，还可基于威胁将声誉数据发送到威胁情报云。

[0006] 示范实施例

转向图 1，图 1 是网络环境 10 的示范实施例的简化框图，在网络环境 10 中可实现用于实时定制的威胁防护的系统和方法。网络环境 10 包括威胁情报云 15、事件分析子云 20、传感器 25a-25c 以及主机 30a-30i。传感器 25a-25c 例如可包括遍及网络环境 10 分布的防止入侵系统、网关设备、防火墙、防病毒软件和 / 或其它安全系统以跨越威胁向量从主机 30a-30i 收集信息，威胁向量包括文件、Web、消息和网络威胁向量。威胁情报云 15 一般表示用于从传感器 25a-25c 接收信息并传递从该信息导出的实时的基于声誉的威胁情报的基础设施。事件分析子云表示用于分析由威胁情报云 15 接收的信息的基础设施，以及还可

提供更新服务35，更新服务35能将威胁信息和策略配置更新传递到传感器25a-25c和/或主机30a-30i。

[0007] 图1的每个元件可通过简单的网络接口或通过任何其它合适的连接(有线或无线)来相互耦合，这提供用于网络通信的可行路径。此外，这些元件中的任何一个或更多可基于具体配置需要进行组合或者从架构中移除。网络环境10可包括能够进行用于在网络中传输或接收分组的传输控制协议/互联网协议(TCP/IP)通信的配置。网络环境10还可基于具体需要在适当情况下结合用户数据报协议/IP (UDP/IP)或任何其它合适的协议来操作。

[0008] 在详细描述图1的操作和基础设施之前，提供某些上下文信息以提供可在网络环境10内发生的一些操作的概观。诚挚提供这样的信息并且只用于教导的目的，因此不应以任何方式解释为限制本公开的广泛应用。

[0009] 通常的网络环境包括以下能力：例如使用互联网来与其它网络电子通信、访问连接到互联网的服务器上托管的Web页面、发送或接收电子邮件(即，email)消息或者与连接到互联网的最终用户或服务器交换文件。用户一般期望存储在网络环境中的数据易于得到但免遭未授权的访问。他们还经常期望通信是可靠的且免遭未授权的访问。然而，恶意用户不断开发新的手段来干扰正常操作以及获得对机密信息的访问权。病毒、木马、蠕虫、Bot以及其它恶意软件是用来利用网络或系统中的弱点的工具的常见示例，但设计成通过未授权访问、破坏、公开、修改数据和/或拒绝服务来干扰计算机或网络的正常操作的任何活动都是“威胁”。

[0010] 能部署广范围的对策来应对威胁，包括防火墙、防止入侵系统、网络访问控制以及Web过滤。防止入侵系统(IPS)(还称为入侵检测和防止系统(IDPS))能例如监视网络和/或系统的活动是否有恶意活动或潜在恶意活动以及发送警报。然而，IPS警报可能不总是可采取行动的。许多警报只提供警告信息或指导，即使观察到的事件指示恶意活动，这是因为单个事件可能不足以用合适的置信度来识别攻击。

[0011] IPS通常处于在线(in-line)以便它能例如通过丢弃分组、重置连接和/或阻挡来自源的业务来积极地阻挡检测到的入侵。IPS能使用多个检测方法，包括应用和协议异常、外壳代码(shell-code)检测算法和特征(signature)。例如，基于特征的检测一般包括将特征(即，对应于已知威胁的任何模式)与观察到的事件或活动比较以识别威胁。示范特征是将远程连接建立为根用户的尝试。另一个示例是接收其主题栏和所附文件是已知形式的恶意软件所特有的电子邮件。

[0012] 基于特征的检测在检测已知威胁时可能非常有效，但在检测未知威胁或者甚至已知威胁的细微变化时可能无效。另外，IPS特征倾向于是通用的而一般不是为局部环境定制的。威胁可能只是局部看得见，而不是全局看得见。从全局部署的传感器收集的知识一般不能被有效利用来改进局部安全策略。还经常要求人工调整策略，这可能导致足以允许感染蔓延的延迟。

[0013] 根据本文中描述的实施例，网络环境10能通过提供用于使全局威胁情报和局部威胁情报相互关联以及提供定制的安全策略的系统和方法来克服这些缺点(和其它缺点)。

[0014] 再次参照图1用于说明，主机30a-30i可以是网络元件，这些网络元件意在包括网络设备、服务器、路由器、交换机、网关、桥、负载均衡器、防火墙、处理器、模块或可操作以在网络环境中交换信息的任何其它合适的设备、组件、元件或对象。网络元件可包括任何合适

的便于其操作的硬件、软件、组件、模块、接口或对象。这可包括适当的允许有效交换数据或信息的算法和通信协议。主机 30a-30i 还可以表示其它有线或无线网络节点，如台式计算机、膝上计算机或移动通信设备(例如，iPhone、iPad、安卓设备等)。

[0015] 威胁情报云 15 在一个实施例中是声誉系统，其可以实现为分布式文件系统集群。一般，声誉系统监视活动并基于实体过去的行为来对其分配声誉值或者分。声誉值可表示在从善意到恶意的范围上的不同的可信赖等级。例如，可基于与网络地址进行的连接或源自该地址的电子邮件来为该地址计算连接声誉值(例如，最小风险、未证实、高风险等)。连接声誉系统可用来拒绝带有已知或可能与恶意活动相关联的 IP 地址的电子邮件或网络连接，而文件声誉系统能阻挡具有已知或可能与恶意活动相关联的散列的文件(例如，应用)的活动。威胁情报云 15 可接收来自遍及网络分布的传感器(例如，传感器 25a-25c)的报告，传感器中的一些可以在由分开的实体控制的分开的域中。例如，收集模块可请求传感器向威胁情报云 15 周期性地发送报告，这些报告可匿名发送以保护敏感信息。报告可包括事件信息，如连接的源和目的地址、活动的类型、下载的文件、使用的协议等，以及可以是可采取行动的(例如，改变严重程度的警报)或劝告的(例如，提供可能不可独立采取行动的关于可疑活动的信息)。

[0016] 事件分析子云 20 表示用于在历史上以及近实时地存储、处理和挖掘事件的云基础设施。子云 20 可实现用于数据挖掘警报的启发法以使来自遍及网络分布的传感器(例如，传感器 25a-25c)的信息相互关联并识别新的威胁。可运行长期和短期性能分析(profiling)算法来识别由传感器全局检测的普遍威胁并自动化响应。因此，子云 20 可收集实时警报信息并提供能关于每个传感器进行定制的高级分析和威胁相互关联，这能便于迅速的全局威胁检测。当威胁发生时，实况威胁信息能被发送回传感器。子云 20 可从威胁情报云 15 (其可从传感器 25a-25c 接收作为警报的事件)检索事件，或可直接从传感器 25a-25c 接收事件，并返回结果，这些结果允许威胁情报云调整与新的威胁相关联的声誉数据。另外，子云 20 还可远程地并近实时地自动向传感器 25a-25c 和 / 或主机 30a-30i 提供更新和新的威胁情报。顾客然后可快速并主动地按照这些更新来行动，通过有效利用子云 20 的处理能力和启发法以及全局威胁情报来保护他们的系统。子云 20 还能使策略配置建议有效、自动调整策略或特征集配置和 / 或使其它响应行动有效，以便能以更高的置信度识别或者阻挡新的全局威胁(且不需人工配置)。

[0017] 在某些实施例中，威胁情报云 15 和事件分析子云 20 两者都可实现为云基础设施。云基础设施一般是这样一种环境：允许对能以最小的服务提供商交互来迅速供应(和释放)的计算资源的共享池的按需网络访问。因此，它能提供计算、软件、数据访问以及存储服务，这些服务不要求最终用户知道传递这些服务的系统的物理位置和配置。云计算基础设施能包括通过共享数据中心传递的服务，其可表现为单个访问点。多个云组件，如云 15 和子云 20，能通过诸如消息队列的松散耦合机制相互通信。因此，处理(和有关的数据)不需要位于指定的、已知的或静态的位置中。云 15 和子云 20 可包括能实时延伸现有能力的任何被管理的、被托管的服务。

[0018] 关于与网络环境 10 相关联的内部结构，威胁情报云 15、事件分析子云 20、传感器 25a-25c 和主机 30a-30i 中的每个能包括用于存储将用在本文中概述的操作中的信息的存储器元件。这些设备还可在任何合适的存储器元件(例如，随机存取存储器(RAM)、只读存储

器(ROM)、可擦除可编程 ROM(EPROM)、电可擦除可编程 ROM(EEPROM)、专用集成电路(ASIC)等)、软件、硬件中或者基于具体需要在适当的情况下在任何其它合适的组件、设备、元件或对象中保存信息。本文中论述的任何存储器部件(memory items)应解释为被包括在广义术语“存储器元件”的范围内。可能在任何数据库、寄存器、表、队列、控制列表或存储结构中提供由威胁情报云 15、事件分析子云 20、传感器 25a-25c 或主机 30a-30i 跟踪或发送的信息,所有这些都能在任何合适的时间段(timeframe)被引用。任何这样的存储选择也可被包括在如本文中使用的广义术语“存储器元件”的范围内。

[0019] 此外,威胁情报云 15、事件分析子云 20、传感器 25a-25c 和主机 30a-30i 可包括能够运行软件或算法来执行如本文中论述的活动的多个处理器。处理器能运行与存储器元件相关联的任何类型的指令以实现本文中详细描述的操作。在一个示例中,处理器可能将元素或物品(例如,数据)从一个状态或事物变换为另一个状态或事物。

[0020] 注意,在某些示范实现中,本文中概述的功能可通过在一个或更多有形介质中编码的逻辑(例如,在 ASIC 中提供的嵌入逻辑、数字信号处理器(DSP)指令、将由处理器或其它类似的机器运行的软件(潜在包括目标代码和源代码)等)来实现,该一个或更多有形介质可包括非短暂性介质。在这些情况中的一些情况下,存储器元件能存储用于本文中描述的操作的数据。这包括存储器元件能够存储被运行以执行本文中描述的活动的软件、逻辑、代码或处理器指令。在另一个示例中,本文中概述的活动可以用固定逻辑或可编程逻辑(例如,由处理器运行的软件 / 计算机指令)来实现,以及本文中标识的元件可能是某一类型的可编程处理器、可编程数字逻辑(例如,现场可编程门阵列(FPGA)、EPROM、EEPROM)或包括数字逻辑、软件、代码、电子指令的ASIC,或者是其任何合适的组合。本文中描述的任何潜在处理元件、模块和机器应解释为被包括在广义术语“处理器”的范围内。

[0021] 图 2 是可与网络环境 10 的示范实施例相关联的潜在操作的简化交互图,在网络环境 10 中子云 20 专用于分析来自 IPS 传感器的事件。在 200,IPS 传感器(例如,传感器 25a)可观察指示威胁的活动,如主机 30b 下载带有嵌入 JAVASCRIPT 标签的 PDF 文档。在 205,局部 IPS 可阻挡威胁和 / 或发送局部警报。在 210,还可向威胁情报云 15 报告该事件。在 215,威胁情报云 15 可确定该事件是否与子云 20 中的事件分析有关(例如,报告是从 IPS 接收的)。如果该事件与子云 20 中的分析有关,则威胁情报云 15 可在 220 将事件信息发送到子云 20。在 225 使用各种分析启发法(例如,基于时间、地理位置、声誉等),子云 20 可使该事件与从遍及网络环境 10 分布的其它传感器报告的事件(或者来自同一传感器的随后事件,如带外业务的意外增加)相互关联以识别全局威胁。

[0022] 例如,对于下载具有 JAVASCRIPT 标签的便携文档格式(PDF)文件可设置低严重性警报。局部策略可忽视这样的事件,这是因为它是低严重性警报。然而,可基于从遍及网络的多个传感器接收的报告来确定这样的 PDF 的声誉和来源。通过数据挖掘从分布的传感器报告的事件,可通过使由某一国家、地区或企业中的传感器报告的事件相互关联来将 PDF 文档识别为目标是该国家、地区或企业的威胁。从声誉差的可疑地址下载该 PDF 文件的主机也能被识别。然后能提供建议、指导和策略改变推荐。

[0023] 在 230,子云 20 可生成全局威胁信息并通知在网络环境 10 中或在网络环境 10 的某一段(例如,与某一国家相关联)内的所有 IPS,以及基于威胁相互关联向它们提供定制的安全策略 / 配置建议。定制的安全策略能包括不需要来自管理员的介入而保护网络环境 10

的粒状(granular)响应行动。例如,更新服务 35 可向传感器 25a 提供定制的安全策略,该安全策略通过地址识别被感染的主机(例如,主机 30b),识别数据丢失(如果有的话)的类型并隔离被感染的主机,或者它可以识别应该被阻挡的某一地址。在 235,子云 20 还可向威胁情报云 15 提供结果以补充其它声誉数据。

[0024] 图 3 是示出可与网络环境 10 的某些实施例相关联的潜在操作的简化流程图 300。在具体实施例中,这样的操作可例如由事件分析子云 20 运行。在 305,可接收事件信息。事件信息可例如推送至威胁情报云 15 或从威胁情报云 15 取出。在一些实施例中,事件信息可由网络环境(例如,网络环境 10)各处分布的传感器报告。可在 310 使事件信息相互关联。如果在 315 相互关联揭示威胁,则定制的安全策略可在 320 被发送到传感器中的至少一个。定制的安全策略能部分或全部基于在 315 识别的威胁。声誉数据(其也可部分或全部基于在 315 检测的威胁)可在 320 被发送。例如,事件信息的相互关联可识别与某一网络地址相关联的威胁以及子云 20 可将该网络地址的声誉的更新发送到威胁情报云 15。

[0025] 因此,网络环境 10 可提供显著的优点,其中一些已经被描述了。更具体地,局部安全对策能使用局部调节的策略来基于局部网络的需要提供针对威胁的防护,以及网络环境 10 能将每个局部传感器(即,传感器 25a-25c)连接到一个全局威胁情报网络中。在网络环境 10 中,局部安全对策不再只对最近的威胁反应。关于新的威胁的情报可自动推送到管理系统,从而允许管理系统主动保护网络。另外,网络环境 10 可通过有效利用用于主动调节的基于云的基础设施来显著降低用于安全对策的总拥有成本。

[0026] 注意,利用以上提供的示例,可根据两个、三个或四个网络元件来描述交互。然而,只是为了清楚和示例的目的才这样做。在某些情况下,通过只参照有限数量的网络元件来描述流的给定集合的一个或更多功能性可能更容易。应理解,网络环境 10(及其教导)可易于扩展且能容纳大量组件以及更复杂 / 更高级的布置和配置。还应理解,本文中描述的在 IPS 的具体上下文中的原理可易于延伸到其它类型的网络元件,如网关、防火墙等,或者延伸到主机系统,如防病毒系统。因此,提供的示例不应限制范围或者约束如潜在应用于很多其它架构的网络环境 10 的广泛教导。此外,虽然参考其中操作可与给定网络元件相关联的具体情景进行描述,但是这些操作能在外部实现,或者以任何合适的方式合并和 / 或组合。在某些情况下,可在单个专有的模块、设备、单元等中提供某些元件。

[0027] 还重要的是,注意附图中的步骤只说明可由网络环境 10 运行或在网络环境 10 内运行的一些可能的信令情景和模式。可在适当情况下删除或移除这些步骤中的一些,或者可相当大地修改或改变这些步骤而不脱离本文中提供的教导的范围。此外,这些操作中的若干操作已描述为与一个或更多额外操作同时运行或并行运行。然而,这些操作的定时可变动相当大。前述操作流已被提供用于示例和论述的目的。由网络环境 10 提供巨大的灵活性,因为可提供任何合适的布置、时间顺序(chronologies)、配置和定时机制而不脱离本文中提供的教导。

[0028] 本领域技术人员可能发现大量其它的改变、替换、变化、变动和修改,且本公开意在包括落入所附权利要求书的范围内的所有这样的改变、替换、变化、变动和修改。为了帮助美国专利商标局(USPTO)并另外帮助基于本申请颁发的任何专利的任何读者解释于此附上的权利要求书,申请人希望指出 :申请人(a)并不意在使任何所附权利要求以其在本申请的申请日存在的形式援引 35 U.S.C 第 112 节的第六(6)段,除非文字“用于…的部件”或

“用于…的步骤”在具体权利要求中被特别地使用；以及(b)并不意在通过本说明书中的任何陈述以未在所附权利要求书中另行反映的任何方式来限制本公开。

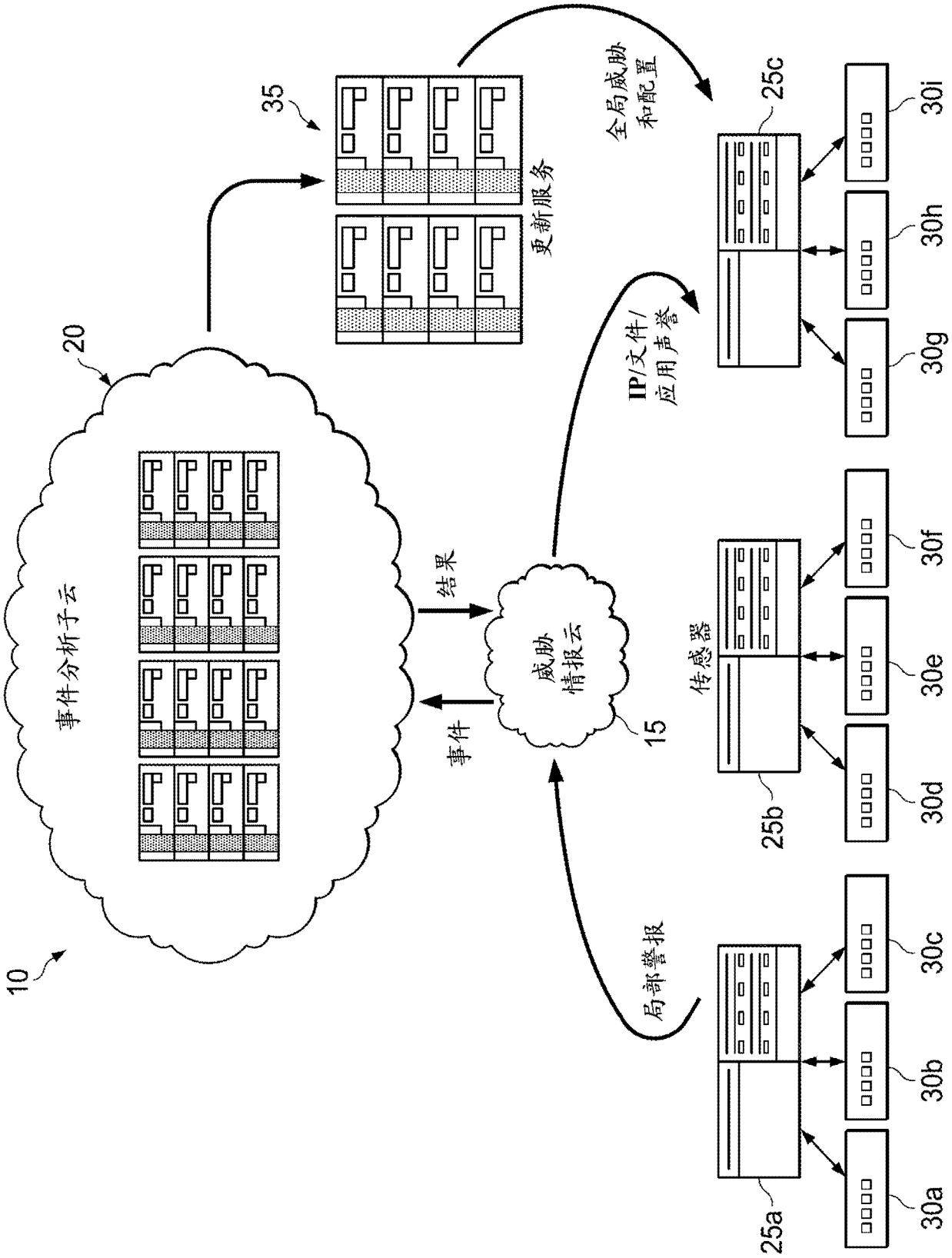

10
20
事件分析子云
35
更新服务
全局威胁
和配置
IP/文件/
应用声誉
结果
事件
威胁
情报云
15
局部警报
传感器
25a
25b
25c
30a
30b
30c
30d
30e
30f
30g
30h
30i

图 1

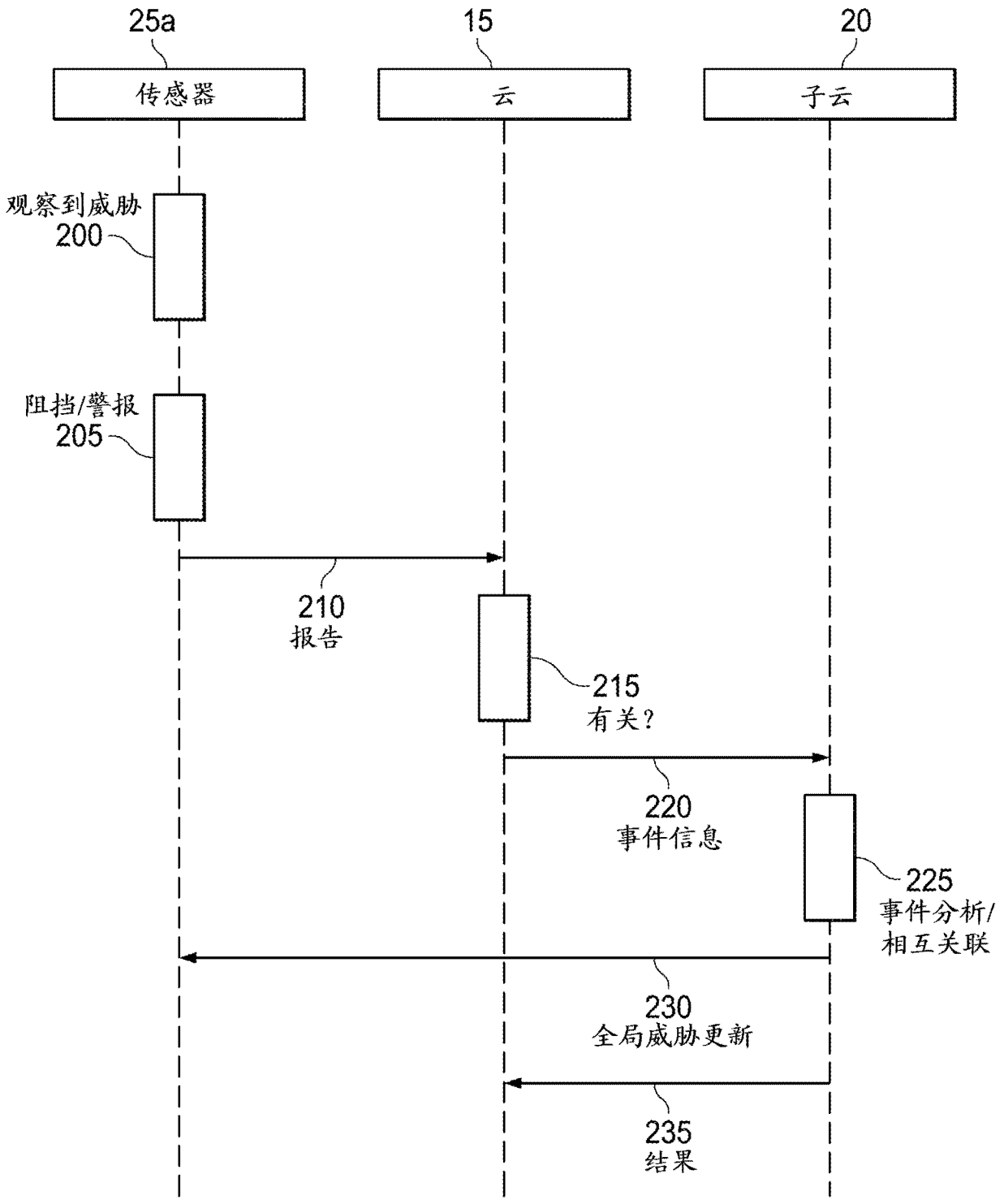

25a
15
20
传感器
云
子云
观察到威胁
200
阻挡/警报
205
210
报告
215
有关?
220
事件信息
225
事件分析/
相互关联
230
全局威胁更新
235
结果

图 2

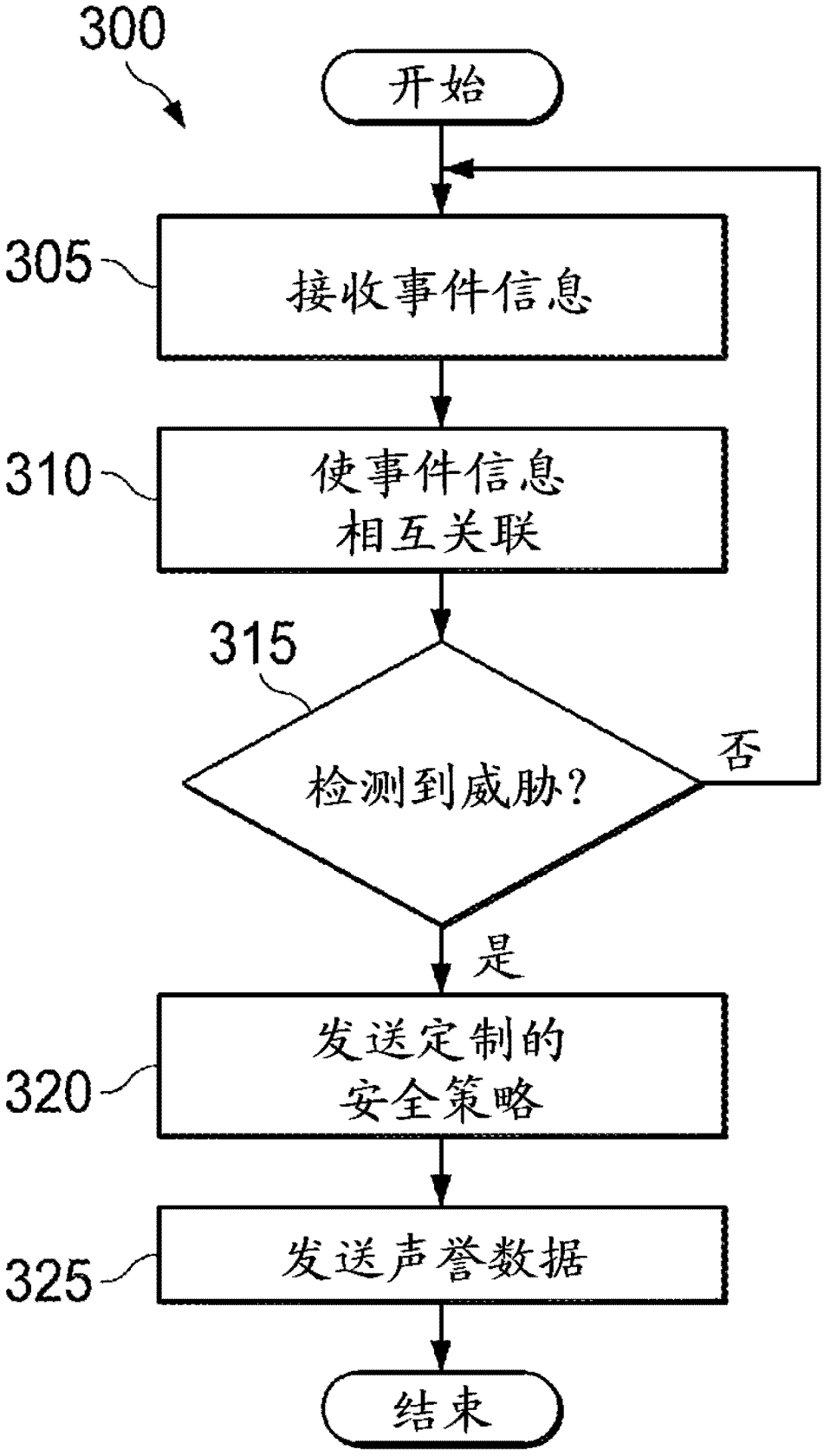

300
开始
305
接收事件信息
310
使事件信息
相互关联
315
检测到威胁?
否
是
320
发送定制的
安全策略
325
发送声誉数据
结束

图 3