发明名称
地理映射系统安全事件

摘要
标识了已经被检测为针对包含在具体计算系统中的具体计算装置的具体安全事件。具体计算系统的多个资产分组中的具体资产分组被标识为包含具体计算装置。还标识了具体安全事件的源，并且地理位置和多个资产分组中的资产分组中的至少一项与标识的源关联。生成适用于使具体安全事件的图形表示呈现在显示装置上的数据。图形表示包含表示在具体资产分组中所包含的具体计算装置的第二图形元素和表示与地理位置和资产分组中的至少一项关联的源的第二图形元素。
1. 一种管理安全信息的方法，所述方法包括：
   标识在具体计算系统中检测的具体安全事件，所述具体安全事件检测为针对包含在所述具体计算系统中的具体计算装置；
   将为所述具体计算系统内的装置定义的多个资产分组中的具体资产分组标识为包含所述具体计算装置；
   标识所述具体安全事件的源，其中所述源与至少一个第二计算装置关联；
   将所述源与地理位置和包含在所述多个资产分组中的资产分组中的至少一项关联；以及
   生成适用于使所述具体安全事件的图形表示呈现在显示装置上的数据，所述图形表示包含：表示在所述具体资产分组中所包含的所述具体计算装置的第二图形元素和表示与地理位置和包含在所述多个资产分组中的资产分组中的至少一项关联的所述源的第二图形元素，
   其中表示与地理位置关联的事件元素的图形元素被叠加在地理位置的视图上来呈现，而表示与资产分组关联的事件元素的图形元素被呈现在所述地理位置的视图的外部。

2. 如权利要求1所述的方法，其中所述图形表示包含地理位置的视图，并且所述第一图形元素和第二图形元素中的至少一个被叠加在所述地理位置的所述视图上。

3. 如权利要求2所述的方法，其中所述源与包含在所述地理位置的所述视图中的具体地理位置关联，并且所述具体地理位置根据与所述源关联的装置标识符标识。

4. 如权利要求2所述的方法，其中所述图形表示进一步包含所述多个资产分组中的两个或更多资产分组的表示，所述两个或更多资产分组包含所述具体资产分组。

5. 如权利要求4所述的方法，其中所述第一图形元素位于与所述具体资产分组的所述表示对应的所述图形表示中，并且所述第二图形元素位于与所述地理位置的所述视图上的所述具体地理位置对应的第一所述图形表示中。

6. 如权利要求1所述的方法，所述图形表示进一步包含图形连接体，所述图形连接体将所述第一图形元素与所述第二图形元素关联，并表示所述具体计算装置和所述源与所述具体安全事件关联。

7. 如权利要求1所述的方法，其中所述第一图形元素是气泡元素，以及所述气泡元素的直径对应于包含所述具体安全事件的检测的安全事件的量。

8. 如权利要求1所述的方法，其中所述源被标识为包含在所述具体计算系统中，并且所述源与所述多个资产分组中的第一分组关联。

9. 如权利要求8所述的方法，其中所述具体资产分组是所述第一分组。

10. 如权利要求8所述的方法，其中所述具体资产分组是不同于所述第一分组的分组。

11. 如权利要求1所述的方法，其中所述图形表示进一步包含所述多个安全事件中的每个事件的表示。

12. 如权利要求1所述的方法，其中所述多个资产分组中的每个资产分组是截然不同的用户定义的资产分组。

13. 如权利要求1所述的方法，其中所述多个资产分组中的每个资产分组对应于所述具体计算系统中资产的IP地址范围。

14. 如权利要求1所述的方法，其中所述图形表示是交互式呈现，并且用户与所述第一
图形元素和第二图形元素中的一个或多个图形元素交互作用使所述具体安全事件的细节视图被呈现。

15. 如权利要求14所述的方法，其中所述用户交互作用包含鼠标移过所述第一图形元素和第二图形元素中的一个或多个图形元素。

16. 如权利要求14所述的方法，其中所述用户交互作用包含选择所述第一图形元素和第二图形元素中的一个或多个图形元素。

17. 如权利要求1所述的方法，其中所述具体安全事件的所述图形表示传达了所述具体安全事件的类型。

18. 如权利要求17所述的方法，其中所述具体安全事件的所述图形表示根据所述具体安全事件的类型对所述第一图形元素和第二图形元素中的每个图形元素进行颜色编码，其中所述具体安全事件的类型是多个安全事件类型之一，并且所述多个安全事件类型中的每个安全事件类型被编码成相应颜色。

19. 如权利要求1所述的方法，其中所述第一图形元素是表示安全事件目标的第一类型图形元素，而所述第二图形元素是表示安全事件源的第二不同类型安全事件。

20. 一种系统，包括执行如权利要求1-19中任一项所述的方法的构件。

21. 一种管理安全信息的设备，所述设备包括机器可执行逻辑，所述逻辑当执行时执行包括如下步骤的操作：

标识在具体计算系统中检测的具体安全事件，所述具体安全事件检测为针对包含在所述具体计算系统中的具体计算装置；

将为所述具体计算系统内的装置定义的多个资产分组中的具体资产分组标识为包含所述具体计算装置；

标识所述具体安全事件的源，其中所述源与至少一个第二计算装置关联；

将所述源与地理位置和包含在所述多个资产分组中的资产分组中的至少一项关联，以及

生成适用于使所述具体安全事件的图形表示呈现在显示装置上的数据，所述图形表示包含表示在所述具体资产分组中所包含的所述具体计算装置的第一图形元素和表示与地理位置和包含在所述多个资产分组中的资产分组中的至少一项关联的所述源的第二图形元素，

其中表示与地理位置关联的事件元素的图形元素将被叠加在地理位置的视图上呈现，而表示与资产分组关联的事件元素的图形元素将被呈现在所述地理位置的视图的外部。

22. 一种管理安全信息的系统，所述系统包括：

至少一个处理器装置；

至少一个存储器元件；以及

地理映射引擎，当由所述至少一个处理器装置执行时适用于：

标识在具体计算系统中检测的具体安全事件，所述具体安全事件检测为针对包含在所述具体计算系统中的具体计算装置；

将为所述具体计算系统内的装置定义的多个资产分组中的具体资产分组标识为包含所述具体计算装置；
标识所述具体安全事件的源，其中所述源与至少一个第二计算装置关联；
将所述源与地理位置和包含在所述多个资产分组中的资产分组中的至少一项关联；以及
生成适用于使所述具体安全事件的图形表示呈现在显示装置上的数据，所述图形表示包含表示在所述具体资产分组中所包含的所述具体计算装置的第一图形元素和表示与地理位置和包含在所述多个资产分组中的资产分组中的至少一项关联的所述源的第二图形元素。
其中表示与地理位置关联的事件元素的图形元素将被叠加在地理地图的视图上来呈现，而表示与资产分组关联的事件元素的图形元素将被呈现在所述地理地图的视图的外部。

23. 一种安全管理信息的方法，所述方法包括：
标识在具体计算系统中检测的具体安全事件，所述具体安全事件检测为涉及包含在所述具体计算系统中的具体计算装置，并且针对在所述计算系统外部的所述至少一个第二计算装置；
将为所述具体计算系统内的装置定义的多个资产分组中的具体资产分组标识为包含所述具体计算装置；
将所述第二计算装置与地理位置关联；以及
生成适用于使所述具体安全事件的图形表示呈现在显示装置上的数据，所述图形表示包含表示为所述具体安全事件的源并且包含在所述具体资产分组中的所述具体计算装置的第一图形元素和表示与所述地理位置关联的所述第二计算装置并叠加在对应于所述地理位置的地理地图的部分表示上的第二图形元素，
其中表示与地理位置关联的事件元素的图形元素被叠加在地理地图的视图上来呈现，而表示与资产分组关联的事件元素的图形元素被呈现在所述地理地图的视图的外部。

24. 一种系统，包括执行如权利要求23所述的方法的构件。
地理映射系统安全事件

技术领域

【0001】一般而言，此公开涉及数据分析领域，并且更具体地说，涉及数据分析软件中的图形用户界面。

背景技术

【0002】计算机安全工具已经被部署遍及全世界，以帮助保护计算系统、装置和资源免于各种威胁、漏洞和风险。由全球资源的不断增长以及国际化带来的恶意软件、病毒、蠕虫、系统漏洞、黑客和威胁的演进继续进行，以跟上计算的进步。因而，也已经增加了对于对抗此类威胁的鲁棒且精密的安全工具的需求。给定此类工具不断增加的复杂性以及管理员可定制它们的安全工具以应对特定威胁（包含对具体装置、系统和应用唯一的威胁）的不断增加的程度，管理和理解一些安全工具的功能性对于几乎所有经验的用户都已经变得太复杂了。管理起来已经变得复杂了，安全工具的一个参考示例是现代网络防火墙。防火墙可以是设计成允许或拒绝进出系统的数据传送（包含通过网络传送的传送）的装置或装置集合，防火墙的操作可基于规则或策略的集合，并且比如可用于保护网络和系统免于非法用户和程序的未授权访问，同时仍允许合法通信。在一些实例中，操作系统也可包含基于软件的防火墙以保护对应系统或主机免于各种威胁，诸如通常经由因特网发现和传递的威胁。

附图说明

【0003】专利或申请文件含有用颜色创作的至少一幅图。具有彩图的此专利或专利申请公布的拷贝将由该局在请求和支付必要费用时提供。

【0004】图1是根据至少一些实施例包含安全事件管理和地理映射功能性的示例计算系统

的简化示意图；

【0005】图2是根据至少一些实施例包含示例地理映射引擎的示例系统的简化框图；

【0006】图3A-3D是阐明根据至少一些实施例在系统中检测的示例安全事件的简化框图；

【0007】图4A-4D是阐明根据至少一些实施例的安全事件地理映射的示例用户界面的屏幕截图；

【0008】图5A-5B是阐明与至少一些实施例关联的示例操作的简化流程图。

【0009】各个附图中的相似附图标记和命名指示相似元素。

具体实施方式

【0010】一般而言，在此说明书中描述的主题的一个方面可用包含标识在具体计算系统中检测的具体安全事件的动作的方法实施，具体安全事件检测为针对包含在具体计算系统中的具体计算装置。为具体计算系统内的装置定义的多个资产分组中的具体资产分组可被标识为包含具体计算装置。可标识与至少一个第二计算装置关联的具体安全事件的源，并且地理位置和包含在多个资产分组中的资产分组中的至少一项可与具体安全事件的源关联。
可生成适用于使或让具体安全事件的图形表示呈现在显示装置上的数据，图形表示包含表示在具体资产分组中所包含的具体计算装置的第一图形元素和表示与地理位置和包含在多个资产分组中的资产分组中的至少一项关联的源的第二图形元素。

[0011] 进一步说，在另一通用方面，可提供包含至少一个处理器装置和至少一个存储器元件和地理映射引擎的系统。地理映射引擎当由处理器执行时可标识在具体计算系统中检测的具体安全事件（具体安全事件检测为针对包含在具体计算系统中的具体计算装置），为具体计算系统中的装置定义的多个资产分组中的具体资产分组标识为包含具体计算装置，标识具体安全事件的源，将源与地理位置和包含在多个资产分组中的资产分组中的至少一项关联，并生成适用于使具体安全事件的图形表示呈现在显示装置上的数据。图形表示可包含表示在具体资产分组中所包含的具体计算装置的第一图形元素和表示与地理位置和包含在多个资产分组中的资产分组中的至少一项关联的源的第二图形元素。

[0012] 进一步说，在此说明书中描述的主题另一方面中可用包含标识在具体计算系统中检测的具体安全事件的动作的方法实施，具体安全事件检测为涉及包含在具体计算系统中的具体计算装置，并且针对在计算系统外部的至少一个第二计算装置。为具体计算系统内的装置定义的多个资产分组中的具体资产分组可标识为包含具体计算装置。第二计算装置可与地理位置关联。此外，可生成适用于使或让具体安全事件的图形表示呈现在显示装置上的数据，图形表示包含表示作为具体安全事件源并且包含在具体资产分组中的具体计算装置的第一图形元素和表示与地理位置关联的第二计算装置并叠加在对应于所述地理位置的地图的图示表示上的第二图形元素。

[0013] 这些以及其它实施例可各可选地包含一个或多个如下特征。图形表示可包含地理地图的视图，并且第一图形元素和第二图形元素中的两个可叠加加在地理地图的视图上，所述源可与包含在地理地图的视图中的具体地理位置关联，并且具体地理位置可根据与所述源关联的装置标识符标识。图形表示可进一步包含多个资产分组中的两个或更多资产分组的表示，两个或更多资产分组包含具体分组。第一图形元素可位于与具体分组的表示对应的图形表示中，并且第二图形元素位于与地理地图的视图上的具体地理位置对应的图形表示中。图形表示可进一步包含图形连接体，所述图形连接体将第一图形元素与第二图形元素关联，并表示具体计算装置和所述源与具体安全事件关联。第一图形元素可以是气泡（bubble）元素，并且气泡元素的直径对应于包含具体安全事件的检测的安全事件的量。图形表示可进一步包含多个安全事件中的每个事件的表示。第一图形元素可包含表示安全事件目标的第一类型图形元素，而第二图形元素可以是表示安全事件源的第二不同类型安全事件。

[0014] 进一步说，实施例可各可选地包含一个或多个如下特征。所述源可被标识为包含在具体计算系统中，并且所述源可与多个资产分组中的第一组分关联。具体分组可以是第一分组，或者不同于第一分组的分组。在一些实施例中，资产分组可以是截然不同的用户定义的资产分组，而在其它实施例中，资产分组可以对应于具体计算系统中资产的IP地址范围。图形表示可以是交互式呈现，并且用户与第一图形元素和第二图形元素中的一个或多个图形元素交互作用可使具体安全事件的细节的视图被呈现。用户交互作用可包含像鼠标移过第一图形元素和第二图形元素中的一个或多个图形元素、选择第一图形元素和第二图形元素中的一个或多个图形元素这样的动作，以及其它动作。具体安全事件的图形表示可进一步传
达具体安全事件的类型。比如，图形表示可根据具体安全事件的类型对第一图形元素和第二图形元素中的每个图形元素进行颜色编码，所述具体安全事件的类型是多个安全事件类型之一，多个安全事件类型中的每个安全事件类型被编码成相应颜色。

【0015】其中一些或所有特征可以是计算机实现的方法，或者进一步包含在用于执行这个所描述功能性的相应系统或其它装置中。在附图和如下描述中阐述了本公开的这些以及其它特征、方面和实现的细节。本公开的其它特征、目的和优点根据说明书和附图以及权利要求书将显而易见。

【0016】示例实施例

【0017】图1是阐明包含由一个或多个安全工具108监视的计算装置（例如105、125、130、135）的系统的计算系统100的示例实现的简化框图。这些安全工具108中的一些可驻留在系统服务器105、网络、网络接口和装置125、130、135上，而其它安全工具108比如可使用远离由工具监视的系统服务器105的计算装置和基础设施提供为服务。系统100可进一步包含分析服务器110、策略管理服务器115以及结合监视系统服务器105的一个或多个安全工具108提供的安全事件检测服务器120。用户端点装置（例如125、130、135）也可提供在系统100中。在一些实施例中，一个或多个端点装置（例如125、130、135）可与之交互作用，并消耗由系统服务器105以及其它服务器和装置（例如万维网服务器140）通过一个或多个网络150托管的服务和资源。在一些实施例中，一个或多个端点装置（例如125、130、135）以及分析服务器110、策略管理服务器115和安全事件检测服务器120中的一个或多个可被视为包含在包含系统服务器105的计算装置系统（诸如企业软件系统）内。进一步说，在系统中实现的一些安全工具可部署在端点装置125、130、135以及实现分析服务器110、策略管理服务器115和安全事件检测服务器120中一个或多个的计算装置上，或者以其它方式监视它们。

【0018】用于监视系统以及系统与系统和装置外部（例如万维网服务器140）的交互作用的安全工具108可收集与安全工具的操作和事件、事务处理以及由安全工具监视的系统装置和组件相关的各种数据。安全工具108可包含基于软件和/或基于硬件的工具，包括防火墙（FW）、万维网网关、邮件网关、基于客户端的用户风险评估引擎、主机入侵保护（HIP）工具、网络入侵保护（NIP）工具、防病毒和防恶意软件扫描仪和移除工具、基于主机和/或基于网络的数据丢失防止（DLP）工具、漏洞管理器，系统策略依从管理器、资产关键性工具、安全信息管理（SIM）产品，除此之外还有其它安全工具。安全工具108可部署在一个或多个端点装置（例如125、130、135）、网络元素（例如网络150的）、系统服务器105或具体系统的其它组件上。其中一个或多个所部署的安全工具108可根据规则或策略的对应集合操作并保护系统组件，这些规则或策略比如指示干预、过滤、阻断、监视、事件或告警检测、业务整型或由安全工具108执行的其它安全任务的条件。此外，安全工具108可检测与系统安全和相应安全工具108的操作相关的具体事件，诸如所检测的威胁、网络使用违反、所检测的漏洞、系统使用违反、系统错误、未授权的访问尝试以及其它事件，并且可收集、存储和报告结合事件的监视和检测所收集的数据。使用安全工具108检测的事件本身可至少部分基于安全工具108和所监视的系统规则和策略。

【0019】与所部署的安全工具108的动作和策略相关的安全数据以及与安全事件的监视和检测相关的数据可由具体安全工具收集和保存，基本上独立于由其它安全工具和系统组件收集或保存的其它数据。安全数据可通过一个或多个系统组件标识、类别和聚集，系统组件包
含比如适用于收集、接收或者以其它方式聚集与由一个或多个安全工具采用的安全策
略和规则相关的安全数据的策略管理服务器115。此外，在一些实现中，安全事件检测服务
器120可类似地收集和聚集描述在所监控的系统和组件内由各种安全工具108所检测的条
件以及事件属性的数据。

[0020] 可提供分析服务器110以帮助用户分析和处理诸如通过策略管理服务器115和安
全事件检测服务器120从系统安全工具108收集的数据。分析服务器110可包含数据分析软
件、数据收集软件允许用户查看、分析、过滤、组织、执行分析计算和操作，以及安全事件
(包含由策略管理服务器115、安全事件检测服务器120或者系统100中的其它工具组织的安全
数据)上的其它任务。在一些实现中，分析服务器110或另一装置或子系统可进一步提供用
于基于与事件关联的地理位置分析所检测的事件条件的功能性。由安全工具108收集的数
据可标识或用于(例如由分析服务器110)标识在安全事件中涉及的具体计算装置(例如通
过IP地址或MAC地址或某一其它标识符)。安全事件可包含事件的“源”或其活动已被确定
为安全事件的可能原因的装置(或与装置关联的用户)。安全事件也可包含事件的“目标”，
或以事件为目标或受事件影响或者在事件检测中涉及的装置、网络或子系统。源或目标可
以是所监视系统内的装置、网络或子系统(例如装置105、125、130、135)，或者可以是远离所
监视系统或在所监视系统外部的装置、网络或系统(例如万维网服务器140、一个或多个最
终用户装置(例如125、130、135)。在一些实例中，比如通过在系统100上采用的对可检测
和中断具体装置上的攻击或其它安全事件，并且虽然作为目标的装置可能实际上受安全事
件的影响，但尽管如此，作为目标的装置仍可被确定为“目标”。其它所检测的攻击或安全事
件的影响可能尚未成功阻止，其中受影响的装置仍被视为目标。

[0021] 除了标识在具体检测的安全事件中涉及的具体源和目标装置，分析服务器110或
另一装置或子系统可确定装置的地理位置(例如根据IP地址的地理位置数据库、第三方地
理位置服务或使用其它地理位置技术，包含已知和未来的地理位置技术)。此外，具体系统
或网络(例如对应企业软件系统)内的装置可被标识为属于一个或多个预先定义的分组、IP
地址范围或其它分组子系统。进一步说，分析服务器110可结合图形用户界面(GUI)的的
生成使用，GUI包含安全数据的各种视图和表示，并允许装置(例如125、130、135)的用户执行
由安全工具108生成和收集的安全数据上的分析。此类GUI和分析呈现可包含生成在系统中
检测的安全事件的交互式地理位置图，诸如在下面的多个示例中描述和示出的。

[0022] 一般而言，“服务器”、“客户端”和“计算装置”，包括用于实现或者以其它方式包含
在系统100(例如105、108、110、115、120、130、135、140等)中的计算装置，可包含可操作以接
收、传送、处理、存储或管理与软件系统100关联的数据和信息的电子计算装置。在此文档中
所使用的术语“计算机”、“计算装置”、“处理器”或“处理装置”意图涵盖任何适合的处理装
置。例如，系统100可使用不同于服务器的计算机(包含服务器工具)实现。进一步说，任何、
所有或一些计算装置可适用于执行任何操作系统(包含Linux、UNIX、Windows服务器等)以
及适用于虚拟化具体操作系统(包含定制和专有操作系统)的执行的虚拟机。

[0023] 进一步说，服务器、客户端和计算装置(例如105、108、110、115、120、125、130、135、
140等)可各包含一个或多个处理器、计算机可读存储器以及一个或多个接口，除此之外还
有其它特征和硬件。服务器可包含任何适合的软件组件或模块，或者能够托管和/或服务于
软件应用或服务(例如分析服务器110的服务)(包含分布式企业或者基于云的软件应用、数
据和业务）的计算装置。比如，服务器可配置成托管、服务或或者以其它方式管理数据集，或与其它服务对接、协调或依赖于其它服务或由其它服务使用或应用，包含聚焦安全的应用和软件工具。在一些实例中，服务器、系统、子系统或计算装置可实现为可在公共计算系统、服务器、服务器池或云计算环境下托管并共享计算资源（包含共享的存储器、处理器和接口）的装置的某种组合。

端点计算装置（例如125、130、135）可包含膝上型计算机、平板计算机、智能电话、个人数字助理、手持视频游戏控制台、台式计算机、因特网上能的电视以及能够通过一个或多个网络150与其它计算装置（包含分析服务器110和/或系统服务器105、万维网服务器140或其他远程装置和子系统）通信并结合其它计算装置操作的其它装置。端点计算装置125、130、135的属性从装置到装置可有很大不同，包含操作系统以及加载的、安装的、执行的、操作的或者以其它方式由装置可访问的软件程序的集合。装置的程序集可包含操作系统、应用、插件、小程序、虚拟机、手机程序、可执行文件以及能够由相应装置（例如125、130、135）运行、执行或者以其它方式使用的其它基于软件的程序。其它装置属性也可包含连接到装置或者以其它方式由该装置可访问的外设装置，以及该装置适用于的网络技术类型。

每个端点计算装置可包含一个或至少一个图形显示装置和用户界面，允许用户通过访问分析服务器110查看在系统100中提供的应用和其它程序的图形用户界面，并与之交互作用。一般而言，端点计算装置可包含可操作以接收、传送、处理和存储与图1的软件环境关联的任何适当数据的任何电子计算装置。将理解，可能存在与系统100关联的任何数量的端点装置以及系统100外部的任何数量的端点装置。进一步说，术语“客户端”、“端点装置”和“用户”视情况而定可互换使用，没有脱离此公开的范围。然而，虽然每个端点装置可在由一个用户使用的方式描述，但公开考虑了许多用户可使用一个计算机或者一个用户可使用多个计算机。

虽然图1被描述为含有多个元素或与多个元素关联，但并不是在图1的系统100中阐明的所有元素都可用在本公开的每个备选实现中。此外，本文描述的一个或多个元素可位于系统100外部，不过在其它实例中，某些元素可被包含在一个或多个其它所描述元素的一部分以及在所阐明的实现中未描述的其它元素内，或作为一个或多个其它所描述元素的一部分以及在所阐明的实现中未描述的其它元素。进一步说，在图1中阐明的某些元素可与其它组件组合，以及用于除本文描述的那些目的之外的备选或附加目的。

尽管向计算系统和资源提供了关键保护，但现代安全工具可能难以管理和准确地部署。对于大企业和系统，本文中部署的防火墙、策略依从、防恶意软件和其他安全工具可由为企业的系统和安全工具的潜在无限性和各样的问题和使用而潜在制定的策略和规则的高速（dizzying）地控制。全球企业可能遭受在多个且多样地理区域中监视装置和子系统的附加复杂性。一些安全风险和问题对于一些物理位置比其它物理位置可能更突出。

评估安全事件，开发响应性安全和企业策略并实现安全工具和对策以确保系统免于此类威胁和漏洞可能是困难的任务。为了阐明一个示例，在企业中部署的防火墙可被派生阻断“坏”业务通过（即进入或退出）同时仍允许企业的好（并且重要）业务自由流动的任务，除此之外还有其它功能。获得这个可涉及定位管控什么业务被允许或阻断、何时这么
做、谁（即哪些用户）允许或拒绝、在什么条件下允许或阻断业务的成千上万的粒度规则和策略，除此之外还有其它因素。例如，防火墙规则可根据具体业务的源或目的地而改变（例如，服务器或客户端的位置是否影响与业务关联的风险，具体用户（例如高级行政主管、HR人员、IT人员）的角色是否可允许其它用户未持有的某种信任或权限等），除此之外还有其它示例。

[0029] 进一步说，在一些现代企业网络中，再网络内寻址主机装置已经被不一致地执行了，其中将IP地址任意指定为主机的一些企业被添加到网络上。其它不一致性也存在，添加组织破坏程度以管理现代企业系统。一般而言，标识并弄懂系统内某些检测的安全事件的重要性可能是困难的，特别是当管理员缺乏标识在事件中影响或涉及系统部件（例如具体办公室、装置类型等）的便利方式时。管理员设法和理解影响系统的事件的能力可阻碍有效地诊断和解决由事件利用的原因和漏洞，快速隔离受影响的资产和子网，并发起适当的对策来解决所检测的事件，除此之外还有其它示例。

[0030] 管理策略、事件和资产的这个万维网以及系统中安全工具的类似复杂的万维网可能是个挑战，特别是当系统安全中出现不一致时。传统安全解决方案虽然尝试通过安全管理给用户提供粒度控制，但经常能它们自己的解决方案、GUI和安全管理工具的对应复杂性压倒几乎最富有经验的用户。用于管理系统内安全性（包含安全事件和策略的整合，诸如图1和图2中所概括的）的系统可解决这些问题，除此之外还有其它问题。

[0031] 转到图2，示出了包含提供地理射频引擎205和事件管理引擎210的示例分析服务器110的示例系统的简化框图200。分析服务器110可提供数据和服务并与之通信以用于开发GUI并将GUI再现现在由用户用于分析系统（例如包含端点装置212、215、220、网络150、服务器230、240中的一个或多个，除此之外还有其它装置或系统组件）的安全条件的端点装置212、215、220上。此类GUI可包含所检测安全事件的地理射频，类似于在下面示出和讨论的（例如结合图4A~4D）。由分析服务器110生成和提供的GUI可进一步包含由部署系统在系统上的一个或多个安全工具（例如225）收集的或与之相关的安全数据的交互式表格、图形、信息图形以及其它图形表示。用户可与显示在端点装置（例如212、215、220）上的GUI交互作用，并执行分析任务，包含以其原始形式以及部分由分析服务器110并且部分由操作在相应端点装置（例如212、215、220）的软件生成的数据的组织和图形表示过滤、检查、比较、分类、分等级和分析安全数据。

[0032] 在一个具体示例实现中，分析服务器110可包含一个或多个处理器装置250和一个或多个机器可读存储器元件255用于执行一个或多个软件程序，至少包含地理射频引擎205和事件管理引擎210的一部分。地理射频引擎205的示例实现可与由事件管理引擎205生成或以其它方式提供的数据对接，并利用这些数据。在一些实现中，事件管理引擎205可包含多个组件和功能，诸如策略管理器260、事件管理器265、GUI管理器270和策略编辑器275，除此之外还有其它潜在组件。在一些实现中，地理射频引擎205和/或事件管理引擎210的一个或多个组件可被分布并提供在基于客户端的分析应用上，诸如安装在端点装置210、215、220上的分析应用。

[0033] 策略管理器260可收集和提供与在系统中一个或多个安全工具的操作相关的安全策略的数据和分析支持。策略管理器可拖拉（pull）、收集或者以其它方式访问在策略管理服务器115聚集的或者直接来自一个或多个对应安全工具225的数据。此数据中的一些可从
为系统保存的数据对象295中导出。系统数据对象295可包含定义系统内关系和属性的数据结构，诸如用户、用户分组、办公室、部门、位置、计算装置、软件应用和应用归类、系统分组以及其它真实世界属性，人、位置、程序、商业实体、组织、装置以及与系统相关的其它东西。策略管理器260可管理一个或多个数据库和/或其它数据结构（例如285），包含标识策略及相关数据，其控制一个或多个安全工具配置225并描述策略和规则的属性。策略数据库285可包含这样的信息：策略的名称、地址或其它标识符；具体策略适用于的地理位置或者策略如何不同地适用于不同地理位置；它适用于的安全工具；由策略控制的安全工具动作的类型或类别；根据策略受安全工具控制、监视和/或保护的应用、组件和/或装置；受策略控制的装置或用户的分组；策略的重要性或关键性的指示；由策略违反触发的告警或事件的类型，除此之外还有其它策略属性。

【0034】事件管理器265可收集和提供数据，并提供与在系统中（例如在安全工具225）检测的事件(包含作为具体策略违反所触发的事件)相关的分析支持。策略管理器可拖拉、收集或者以其它方式访问在安全事件检测服务器120聚合的或者直接来自一个或多个对应安全工具225的数据。事件管理器265可管理一个或多个数据库和/或其它数据结构（例如290），包含标识所检测安全事件的属性和特性的所聚集安全事件数据。此数据中的一些可从系统对象295中导出。此类安全事件数据可包含事件的标识符；在安全事件中涉及的装置或子系统（以及装置的位置、用户或管理器）；所检测的事件数量；检测事件的时间；触发事件的策略违反的标识；什么行动、程序或计算资源违反策略；与安全事件关联的逻辑系统分组（例如部门、商业单位、装置类型等）；安全事件发生的最后时间的标识，或描述先前安全事件检测的其它历史数据；事件的关键性或严重性；事件是否已经被补救或指派给票据、IT专业人员等以便解决；除此之外还有其它示例。

【0035】除了分别管理策略数据和安全事件数据，策略管理器260和事件管理器265可各提供为在其上执行具体分析操作并基于对应的策略数据285和事件数据库290结合GUI管理器270提供GUI呈现和图形表示而特有的附加功能。进一步说，GUI管理器270可整合GUI元素，诸如窗口、窗格、图形表示、控制以及不同上下文（包含以策略为中心的上下文和以事件为中心的上下文）的其它GUI元素。进一步说，GUI管理器270可结合映射标识的安全事件和相关事件属性（例如对应的策略、由系统对象295定义的属性等）到如交互式地图GUI上的地理位置的GUI的生成与地理映射引擎205对接，提供用于地理映射引擎205的功能性，或者与地理映射引擎205协作操作。使用GUI管理器270生成的GUI可包含多个不同上下文，比如组合了聚焦地理的上下文与一个或多个其它上下文，诸如基于事件的事件上下文、以策略为中心的上下文等。一般而言，上下文可对应于通过其比如可在分析操作、GUI或其它分析应用特征中查看、组织或表示具体数据的逻辑类别、对象或主题。事实上，用户可与第一上下文（即以地理为中心的上下文）提供的一个或多个GUI交互作用，结合执行此第一上下文内的一个或多个分析操作，并且然后发起呈现在第二上下文（即以策略为中心或基于事件的上下文、以事件为中心的上下文）中的附加GUI元素的生成和/或呈现。在所呈现的GUI中呈现的GUI元素可进一步示出在一个上下文中的交互作用如何与另一上下文相关。在一些实施例中，GUI管理器270可提供这种整合。

【0036】作为简化的示例，用户可查看安全事件集合的列表、信息图形或其它图形表示（即在以事件为中心的上下文中）。用户可执行过滤、分级、分类、搜索、联结、计算以及其它分析
操作，这些操作导致标识描述安全事件的数据的不同集合，诸如安全事件集合的所选子集，或基于安全事件数据的计算结果。在一些实例中，以事件为中心的列表的生成本身可响应于用户与另一GUI窗口的交互作用生成，诸如事件到图的地理映射。与图窗口中的GUI元素交互作用可使包含在列表中的事件的列表根据交互作用进行过滤。

[0037] 在其它实例中，以策略为中心的GUI窗口和元素可被呈现并且包含以策略为中心的信息、图形表示、信息图等，描述每一个标识策略的属性以及以策略为中心的分析操作（例如对安全策略数据分析特定的过滤、分级、计算、组织等）。进一步说，对具体上下文，可特制提供在具体上下文中的GUI控制。比如，在以策略为中心的GUI元素中提供的给用户提供发起编辑在以策略为中心的GUI元素中标识的其中一个或多个安全策略的能力的交互式GUI工具的一个集合（诸如按钮或其它控制）在另一上下文中可能不可用。比如，可提供策略编辑器275，使能够例如结合一个或多个安全工具的监视、质量控制、部署和维护来编辑安全策略参数。事实上，整合以策略为中心的上下文和以事件为中心的上下文的GUI可为用户提供用于标识、诊断和补救系统中与策略和事件相关的问题的工具的工作流程。采用比如由策略编辑器275提供的功能的从类似GUI进行和发起的修改可影响并修改在系统中部署的安全工具225的变化操作。

[0038] 转到图3A-3D,示出了阐明所监视计算系统内潜在安全相关事件的简化框图。比如，在图3A中，示出了计算装置（例如305、310、315、320、340、345、350、355等）的系统。其中一些计算装置（例如305、310、315、320）可被包含在特定计算的计算系统（例如企业系统）中，并且进一步使用企业网325与其它装置（例如305、310、315、320、340、345、350、355等）对接和通信。可提供监视具体系统的内的事件和活动（包含在装置305、310、315、320以及企业网325的活动）的安全工具（未示出）。安全工具在它们监视具体系统的过程中可确定或检测具体安全相关事件，包含基于为具体系统定义的具体安全策略的事件。

[0039] 具体系统内的计算装置（例如305、310、315、320）可具有由系统使用的对应标识符，包含IP地址、MAC地址、用户ID、序列号、跟踪号等。在一些实例中，检测具体系统内的事件可包含将在检测的事件中受影响或以其它方式涉及的那些装置与事件关联。进一步说，系统内的装置可与在所监视系统内定义的装置和子系统的具体分组关联。此类分组可被创建为系统的功能（例如通过IP地址范围或某种其它自动或任意选择的属性对装置分组），而其它分组可能是更具逻辑性的，诸如通过所定义的用户分组、办公室、型号、装置类型等分组的装置。逻辑分组可反映组织的内部商业逻辑、所分组的装置之间的功能关系或某种其它第二阶逻辑。逻辑分组可包含用户定义的分组，并且可独立于机器标识符，诸如装置的IP地址或MAC地址，除此之外还有其它示例。因此，具体系统内的计算装置（以及它们的具体地址信息）可通过IP地址范围或某种其它定义的属性而映射到一个或多个装置分组。

[0040] 在图3A的示例中，具体系统中的装置可根据每个装置的相应IP地址落入的IP地址范围进行分组。比如，装置305和310可被分组在第一IP地址范围（例如落在开始于“10.1”到“10.15”的IP地址之间的地址），同时标识包含装置315、320的第二IP地址范围（例如“10.16”以及更高）。

[0041] 应该进一步指出，如图3A-3D中的每个图中所示的，系统外部的装置如可通过每个装置（例如340、345、350、355）的相应IP地址的地理位置分析或另一地理位置技术各个标识为位于具体地理位置或者以其其它方式与之关联。例如，可以标识，一些外部装置或系统
340、350（例如未包含在诸如企业系统的所监视系统中的装置）比如位于中国，而其它装置和系统被标识为位于美国或其它地区和区域或者与之关联。进一步说，在一些实例中，所监视系统以及所监视网络（325）内的装置305、310、315、320可以不位于同一位置，并且可分散在多个办公室、国家、州和省等。因而，在一些实际中，还可能确定所监视系统内的各种装置305、310、315、320的相应地理位置，以及所监视系统内的装置305、310、315、320的任何其它逻辑分组或任意分组。

【0042】继续图3A的示例，可标识具体系统安全相关事件（例如360）。在一些实例中，如图3A的示例中所示，事件可以是系统间事件，因为它涉及系统内包含的源装置（例如310）和目标装置（例如320）。作为示例，安全事件360可涉及具体最后用户源装置310通过企业网325（例如基于指示使用装置310和320之一或二者以及企业网325的一个或多个策略）尝试的事件为对目标系统服务器装置320的未授权访问或在目标系统服务器装置320上执行未授权的有风险或否则不适当的活动。还可能检测其它系统间事件，包含涉及系统装置305、310、315、320和/或企业网325的任何组合的系统间事件。

【0043】转到图3B，阐明了涉及所监视系统（例如包含305、310、315、320、325）的不同安全相关事件365。在图3B的具体示例中，在所标识的安全事件365中可涉及一个或多个装置（例如340、345、350、355）或网络（例如公用网335，诸如因特网）。当事件（例如365）涉及所监视系统的装置（例如系统服务器320）和所监视系统外部的至少一个装置或用户（例如最终用户装置355）时，事件可被视为系统内事件。

【0044】在图3B的具体示例中，外部装置（例如355）可尝试黑客行为，赢得未授权访问、安装恶意软件或执行针对、影响、损害、威胁或作用（统称为“针对”）所监视的系统服务器320的另一动作（例如365），其被认为是根据一个或多个安全策略的安全事件。在此具体示例中，外部装置355是事件的源，而所监视的系统装置320是目标。在其它示例（诸如图3C的示例）中，系统内安全事件365可涉及检测事件370，其涉及由具体监视的系统内的源装置（例如310）针对外部装置（例如服务器340）的未授权活动。

【0045】在图3A-3C的示例中，可检测涉及源装置和目标装置的安全事件。进一步说，可以确定所监视系统的外部的目标装置和源装置的相应地理位置，以及与包含在所监视系统中的装置关联的相应系统分组。例如，结合图3B的具体示例，可以确定已经检测到涉及由标识为中国（作为示例）的另一装置或系统（例如355）对包含在“IP地址范围2”中的系统装置（例如320）的攻击的安全事件。进一步说，在图3C的具体示例中，可检测到事件源（例如装置310）留在“IP地址范围1”内，该事件影响或针对标识为位于美国的外部装置。在一些实例中，比如可在所生成的GUI中收集和利用这个信息以呈现相关事件（例如360、365、370）的信息，包含事件到交互式地图GUI上的地理映射。

【0046】如上所述所指出，可以代替或附加基于根据装置的相应标识符诸如通过IP地址（与图3A-3C中的示例一样）使用各种技术对所监视系统内的装置305、310、315、320进行分组。为了阐明，在图3D所示的一个示例中，可以代替或附加用于通过IP地址范围引用在所检测安全事件中涉及的系统装置根据一个或多个备选分组（例如“分组1”、“分组2”、“分组3”）来进行分组。进一步对系统装置进行归类或引用。比如，在一些实现中，可根据用户定义的分组，诸如根据装置类型、位置、操作系统、装置拥有者、装置管理者等对装置进行归类。如图3D所示的，事件365的目标装置320（图3D的示例）可被标识为不仅包含在具体IP地址范围（例如IP
地址范围2)中，而且(或者替代之)可被标识为包含在一个或多个备选分组(例如分组3)中。

[0047] 转到因4A-4D，示出了至少部分通过地理映射引擎的功能性例如结合分析服务器
和/或一个或多个安全分析程序的功能性而提供的示例用户界面的屏幕截图400a-d。屏幕
截图400a-d被提供为可能GUI的示例，提供具体检测的事件(例如在图3A-3D的示例中示出
和描述的事件类型)的地理上下文的视图，以及在一些实例中提供与所检测事件相关的那
些策略。转到图4A，示出了阐明示例GUI窗口405的屏幕截图400a，GUI窗口405呈现了与表示
所监视系统内计算装置分组的图形元素(例如410a-c)以及表示涉及所监视系统的所检测
安全事件的附加图形元素(例如420,422,424,426,428,430,432,440,442,444,446,448,
450,452)叠加的交互式地图。交互式地图GUI 405的图形表示可进一步包含交互式GUI工
具，诸如工具415，其适用于允许用户对显示在GUI 405中的地图的具体视图进行放大或缩
小。在一些实现中，在将特征呈现在触摸屏装置上的情况下，用户可隐式或显式控制。地图GUI
405的其它功能性可包含如下能力：搜索具体地理位置并在所显示的地图上标识对应位置，
拖曳所示的地图视图以平移到备选地图视图，以及以其它方式查看和控制在地图GUI 405中
呈现的(或能够呈现的)可用地图视图的变化部分(或其所有)的视图。

[0048] 表示所检测安全事件的多个图形元素(例如420,422,424,426,428,430,432,440,442,
444,446,448,450,452)可呈现与在相应安全事件中受影响或以其它方式涉及的装置和系
统相关的信息。比如，元素420可对应于检测为影响或针对监视系统中一个或多个装置的
安全事件的所标识源的位置。在图4A-4D的具体示例中，提供了两种不同的图形元素类型，
一种表示安全事件的所标识“源”(例如空心圆元素，诸如元素420,422,424,426,428,432)；
而第二种表示安全事件的“目标”(例如实心圆元素，诸如元素440,442,444,446,448,
450,452)。进而说，一个或多个事件的源元素(例如用空心圆示出的)可凭借所选源元素(例
如分别是424,432)连接到对应目标元素(例如分别是444,430)的连接体。具体元素(例如453,454)用
图形表示为与一个或多个对应目标关联。

[0049] 进一步说，比如，单次可在单个地图GUI视图(例如405)中显示多个元素(例如420,
422,424,426,428,430,432,440,442,444,446,448,450,452)以表示在具体时段上在所监视系统内检测
的安全事件的总数的总子集或过滤的子集。比如，可基于(例如由在给定视图中显示的图
表GUI的一部分表示的)具体地理区域的标识，根据安全事件基于的某些安全策略的子集，安全事件类型的子集，由用户来过滤在地图GUI视图405中呈现的安全
事件(例如过滤所检测事件的集合)以示出具体用户管理员负责监视和解决的事件(除此之外
还有其它示例)。

[0050] 表示计算装置分组的图形元素410a-c可基于计算装置的一个或多个具体分组的
自动或用户选择而再现地图GUI 405上，比如，用户可选择执行具体不可通过IP地址范
围、系统内计算装置的类型(例如所有膝上型、所有基于Windows *的机器等)、与具体用户
(例如装置拥有者、装置的注册用户或任务是监视装置安全的管理员等)关联的装置以及其
它分组的分析。对应的资产分组(以及构成装置)可被标识(例如通过IP地址、MAC地址或到
资产分组的其它映射)，并且再现和呈现的图形元素(例如410a-c)叠加在地图GUI视图405
上。在一些实例中，图形元素410a-c的相对大小可被再现以反映分组的相对大小(例如分组
内的装置数量)，或者以其它方式优化用于表示资产分组和事件。比如，图形元素410a-c的
跨度可基于在对应资产分组内检测的事件数量进行优化，其中提供了更大跨度(或图形元
素面积)以容纳呈现在图形元素410a-c上的若干事件元素(例如432,440,442,444,446,448,450,452)。进一步说，虽然在图4A、4B和4D的示例中示出了单行图形元素410a-c，但在其它实例中，可提供多行图形元素(例如410a-c)以结合地图GUI视图405表示所分析的资产分组。在一些实例中，具体装置或装置群集可属于由资产分组元素410a-c表示的多个分组，并且对应资产分组元素(和/或事件元素)可被再现以表示资产分组的这些交互作用或叠加。

【0051】虽然地图GUI视图405上的事件图形元素(例如420,422,424,426,428,430)的放置的位置可对应于所表示事件的具体地理位置，但在一些实现中，呈现为图形元素410a-c上的事件元素(例如442,444,446,448,450,452)的放置可表示比在具体分组的对应事件的涉及多。比如，图形元素410b内的图形元素432,448,450的放置可表示在所表示事件中涉及的装置的相对IP地址(例如其中表示装置或装置群集的元素448由与元素432和450表示的装置相比在IP地址范围“10.16”中具有更低的IP地址)，不过在其它示例中，图形元素410b内的图形元素432,448,450的放置可表示所检测事件的相对年代(例如其中由元素448表示的事件比由元素432,450表示的事件开始或检测)得早。也采用其它约定和术语来指示图形元素410a-c上的事件元素的放置。例如，可根据事件的所确定的严重程度来呈现事件元素(例如432,440,442,444,446,448,450,452)。在其它实例中，事件元素(例如432,440,442,444,446,448,450,452)可以标识为直观地使大多数用户高兴的方式呈现在资产分组元素410a-c上。进一步说，在一些示例中，用户可选项采用该约定用于排序、分类或者以其它方式呈现资产分组元素410a-c，以及在资产分组元素410a-c上排序或呈现事件元素(例如432,440,442,444,446,448,450,452)。例如，用户可选项(或者切换选择)通过相对IP地址、年代次序、严重性等将事件元素(例如432,440,442,444,446,448,450,452)呈现为在资产分组元素410a-c上。在一些实现中，用户可与所呈现的事件元素(例如432,440,442,444,446,448,450,452)交互作用，并将事件元素拖放在对应资产分组元素410a-c内的任何位置，以根据用户的偏好排序或组织所呈现的事件元素，除此之外还有其它示例。

【0052】为了阐明，在图4A的示例中，系统内安全事件可被标识为引起、发起或以其它方式关联位于阿根廷的源装置。叠加在对应于阿根廷的GUI地图部分上的对应图形元素426可表示阿根廷内的源装置的位置。并且进一步指出，安全事件针对或以其它方式影响所监视系统中的目标装置(例如基于位于分组元素410a中的对应图形元素446的放置)。目标装置根据IP地址范围可被标识为包含在装置分组中。在此具体示例中，目标装置可包含在IP地址分组“10.1”中(例如对于IPv4，IP地址开始于“10.1.X.X”)。目标装置属于的分组可由目标图形元素446表示，并且图形元素410a附近或其上的图形元素446放置表示IP地址分组“10.1”。图形元素425和446可进一步用图形表示为连接的，以示出源装置被标识为对应于源自阿根廷(由元素426表示)并且针对具体IP地址分组“10.1”(由元素446表示)中的一个或多个装置的类型安全事件。

【0053】在一些实例中，单个图形元素(420,422,424,426,428,430,432,440,442,444,446,448,450,452)可指的是涉及具体源或目标或者在具体地理位置或系统分组内的源或目标的所检测的多个安全事件。比如，图形元素424和444(包含链接这两个元素的图形连接体)可表示具体时间跨度内具体安全事件或安全事件类型的多个实例或检测，每一个事件实例或检测涉及在葡萄牙建立的源和在所监视系统内的IP地址范围“10.1”分组中包含的
目标。对应于元素424、444、453的组合的每一个事件可以是涉及全部检测为位于葡萄牙国内的同一源装置或多个源装置（例如由元素424单独或共同表示）的事件。类似地，对应于元素424、444、453的组合的事件可以是各个影响或针对IP地址（例如“10.1”）的具体资产分组内的单个装置或多个装置的事件。

[0054] 在一些实例中，单个源元素可被映射到多个目标元素。进一步说，多个目标元素可被映射到多个源元素（例如表示多源攻击，或涉及多个地理区域中的多个源的某种其它安全事件）。作为示例，安全事件从源元素422（表示美国东海岸的源）映射到由元素440、442、452表示的多个系统目标。诸如此类的示例中，将事件映射到多个目标可表示多种事件属性，包含受事件影响的多个截然不同装置、所检测事件的集群等。在系统分组中，集成装置的事件群集（例如包含在第一分组“10.1”中的两个元素440、442）或在具体时域内检测的事件的集群（例如元素440表示在第一时段内检测的事件，元素442表示在第二时段内分组“10.1”中检测的事件）等，以及/或同一类型事件的多个实例（例如两个不同病毒或恶意软件事件源自东海岸但涉及截然不同类型的恶意软件等，影响（例如由元素440和442所表示的同一分组中的装置），除此之外还有其它示例。

[0055] 如上面所指出的，多个不同源或目标可由单个图形元素表示。在一些实例中，受影响装置的数量（或者各选地，具体安全事件或安全事件类型的所检测实例的数量）可在源（或目标）图形元素的特征中表示。比如，如图4A的示例中所示，一些元素（例如442）的直径大于其它元素（例如444）的直径。在一些实现中，叠加在分组元素410a-c或地图GUI 405中的具体图形元素的直径可表示装置（或源/目标）的数量和/或具体安全事件或安全事件类型的所检测实例的数量。比如，基于元素442和444的相对直径，可以标识，已经检测到影响分组“10.1”中资产的更高数量的安全事件源自于美国东海岸，那个事件源自于葡萄牙。

[0056] 附加信息可由地图GUI 405及其构成元素（例如420、422、424、426、428、430、432、440、442、444、446、448、450、452）传达。比如，安全事件可依据各种标准（例如通过事件类型、事件管理员、系统间和系统内事件，除此之外还有其他示例）进行归类。在一个示例实现中，安全事件可通过类型（例如防病毒事件、恶意网站事件、入侵检测事件、恶意可执行事件、混淆通信事件等）进行归类，并且每种类型安全事件可进行颜色编码（即指配具体代表性颜色）。进一步说，共同表示具体类型安全事件实例的源/目标的连接体可各用一个对该颜色呈现。比如，由元素422、424、440、442、444、452等（以及它们的相应连接体）所表示的事件可以是第一类型事件，并在地图GUI 405内呈现为焦绿色。进一步说，由元素430、432、450表示的事件可属于第二类型，并用金色呈现，而第三类型事件（例如由元素426、428、444、448表示的）用蓝色呈现。除此之外还有其它示例。通过使用各种形式的元素（例如源元素和目标元素），调整相应元素的大小（例如基于所检测的事件实例的数量），并改变元素的相应颜色（例如基于事件类型），所检测安全事件的事件的各种（并且可能巨大的）集合的一个特性可被方便地传递给用户，比如帮助用户有效且高效地管理系统或其子系统内的安全。

[0057] 如上面所指出的，在一些实现中，地图GUI 405可以是交互式的，允许用户放大或缩小，平移和滚动以及以其它方式控制呈现在地图GUI 405中的地图视图。进一步说，包含在/或叠加在地图GUI 405上的图形元素（例如420、422、424、426、428、430、432、440、442、444、446、448、450、452）可以是交互式。比如，用户选择具体源元素（例如428）或者鼠标滑过该元素可显示相关或呈现视图（诸如弹出窗口或其它窗口或GUI元素），传递有关
源元素的附加细节，诸如对应事件的类型或性质、所检测事件的数量、最后检测事件的日期、事件的更精确位置（例如事件的城市或州）、指派给事件的管理员、与受事件影响的装置关联的用户，除此之外还有其它细节。可响应于用户与对应目标图形元素（例如448）的交互作用，提供与显示目标或目标分组相关的类似细节。也可与连接体元素交互作用以提供描述相关事件实例的属性的详细视图。进一步说，在一些实例中，选择具体事件相关元素（例如424、444、453）或与之交互作用可使在GUI窗口或事件分析中考虑的安全事件集合被过滤。比如，选择具体交互式图形元素可提示根据事件类型、与事件关联的地理位置、与事件关联的系统分组（例如“10.1”、“10.16”等）(除此之外还有其它示例)过滤事件集合。

与分组元素（例如410a-c）的交互作用也可使事件集合被过滤。例如，选择分组元素410c可过滤结果集合以仅显示、考虑或提供涉及开始于“172.68”的地址范围内的计算资产分组的事件的附加细节。进一步说，在一些实例中，提示所考虑安全事件的集合的对应过滤的与地图GUI 405的图形元素交互作用可进一步导致地图GUI 405的呈现被改变。例如，选择对应于具体国家的图形元素可使得仅显示涉及那个国家的事件。选择对应于具体类型的事件的图形元素可使得在地图GUI 405中仅显示属于所选类型的事件。在另一示例中，选择具体分组元素（例如410a-c）可使未选择的分组（以及对应的图形元素）被由所选分组内的子分组取代（例如选择分组“172.68”可导致分组元素410a-c由对应于“172.68”IP地址范围的子分组（例如“172.68.1”、“172.68.8”等）的新分组元素取代），除此之外还有其它示例。

进一步说，在一些实例中，用户可能期望仅查看对应于系统具体分组的事件。如在图4A的示例中一样，IP范围“10.1”、“10.16”和“172.68”可仅表示所监视系统中的资产（以及对应分配的IP地址）的小子集。在一些实例中，用户可能在系统内预先选择多个资产分组的子集，多个资产分组表示系统中的资产总体。比如，在图4A的示例中，地图GUI 405比如可基于用户事先选择的资产分组“10.1”、“10.16”和“172.68”而生成。类似地，可使用其它标准生成或细化具体地图GUI的呈现，包含事件类型集合、地理位置以及用户选择的其它事件特征（包含根据与地图GUI 405本身交互作用而进行的选择）。

除了响应于用户与地图GUI 405及其构成图形元素的交互作用而改变之外，当检测到附加安全事件并收集到安全事件数据时，地图GUI 405也可动态且自动改变。例如，在图4B中，可在地图GUI 405中检测和呈现由图形元素455、458、459表示的附加事件实例。图4B进一步阐明了系统间事件的示例，诸如涉及威胁或执行涉及由也与系统一起定位的元素450、455、458表示的目标资产的具体活动的一个或多个源（由元素432表示）的事件。进一步说，在一些实例中，具体事件可以从系统间事件和系统内事件，涉及包含在所监视系统的内部（例如在450）和外部（例如在430）的目标，和/或涉及包含在所监视系统的内部（例如在432）和外部（例如在422）的源。

转到图4C，可生成附加GUI窗口（例如460），反映或概括所检测安全事件的地理关系。进一步说，此类地理位置GUI可结合或基于地图的地理位置GUI（诸如图4A-4B的地图GUI 405）呈现。事实上，在一个示例中，地理位置描述GUI 460可结合地图GUI（例如405）呈现，以概括并提供基于地理学的事件GUI上下文的备选视图。

在图4C的示例中，示出了地理位置描述GUI 460的屏幕截图400c，包含安全事件的概括、它们的相应源和目标以及对于所标识源和目标所标识的地理位置和系统分组。地理
位置概括GUI 460的备选视图比如可提供影响具体系统分组并且涉及具体地理位置的安全事件类型的聚集视图。事实上，在图4C的具体示例中，在图4A中的地图GUI 405的屏幕截图400a中映射的事件部分被呈现在地理位置概括GUI 460内。比如，源元素426’（映射位于阿根廷的地图GUI 405的源元素426）被显示在地理位置概括GUI 460中，并与“阿根廷”关联。目标元素446’同样对应于GUI 405的目标元素446，表示受安全事件影响并包含在系统分组“10.1”中的所监视系统的装置和资产。进一步说，概括GUI 460中的表示可使有关事件的源与目标（或目的地）之间的其它图形再现（例如地图GUI 405）中的隐式表示变显式，同时保持在其它呈现中使用的约定（例如空心圆表示源，而实心圆表示事件目标）。进一步说，安全事件（由元素426’、446’表示）的颜色编码可与在对应地图GUI 405中采用的颜色编码一致，例如表示特定类型事件，多个相关事件当中的最相关类型或某种其它容易接近和预测的表示。类似地，在地图GUI 405中表示的其它事件可被映射到地理位置概括GUI 460，如在图4C的示例中所示出的。

【0063】如同图4A和4B的GUI，在地理位置概括GUI 460的一些实现中，构成的图形元素（例如426’、446’、470）可以是可选的或者呈现用户交互式的，并且提示与安全事件管理相关的某些过滤、GUI控制和选择任务。比如，可选择对应于基于阿根廷的事件（在GUI 405中由元素426、446表示）的行元素470，比如以显示呈现由图形元素（例如426’、446’、470）表示的事件的附加细节和属性的窗口，除此之外还有其它示例，包含要呈现在地理位置概括GUI 460和/或地图GUI 405中的安全事件的分类、过滤和选择。

【0064】如上所述的，安全事件的地理位置及相关GUI可以只是用于呈现和评估在所监视系统内检测的安全事件的几个可用上下文之一。如图4D的示例中所示的，在单个GUI内可显示多个GUI上下文，包含地理位置GUI 480（例如包含地图GUI 405和地理位置概括GUI 460），以事件为中心的趋势线GUI呈现485（例如示出在具体事件内检测的安全事件的不同类型量），细节视图GUI 490（例如如基于用户与其它GUI窗口（例如480、485）内的此事件或策略的对应图形表示的交互作用来呈现具体安全事件、安全事件类别、相关安全策略等细节），除此之外还包含其它潜在GUI上下文，包含以策略为中心的GUI窗口和其它窗口。

【0065】如上所述的，用户与一个GUI窗口的交互作用可影响对其它同时呈现实时的GUI窗口的改变。例如，用户选择或与趋势线GUI 485中的 GUI元素（例如492）的其它交互作用可改变或突出另一同时呈现的GUI的呈现，包含呈现地图GUI 450及其构成元素。比如，选择表示在“IDS签名匹配”列表中在8am与9am之间检测的事件的GUI元素492可提示加亮地理位置概括GUI 460中的行元素（例如所标记的阿根廷），以示出在地理位置概括GUI 460行中表示的事件被包含在由GUI元素492表示的安全事件中或者以其它方式与之相关。比如，耦合地理位置GUI（405）与趋势线GUI 485（然而被简化了）可加强分析正在发生的时帧的优先（overriding）的上下文，除此之外还有其它益处。类似地，与地理位置概括GUI 460或地图GUI 405的交互作用可提示其它GUI窗口和GUI（包含同时呈现的GUI窗口）根据用户与地图GUI 405或地理位置概括GUI 460的交互作用进行修改。比如，选择在地理位置概括GUI 460中标记为“阿根廷”的行元素，或选择呈现在地图GUI 405中表示涉及阿根廷的入侵检测（即“IDS”）安全事件的元素（例如426），可进一步提示加亮趋势线GUI 485内（或在地理位置概括GUI 460或地图GUI 405中的另一个中的行或元素（例如492），除此之外还有其它示例。
进一步说，对应安全事件或安全事件子集的细节可基于选择表示安全事件的具体GUI元素来呈现（例如在GUI窗口490中）。用这些各种GUI上下文、用户可通过与一个上下文交互作用并观察交互作用对上下文的影响来控制和评估各种呈现的上下文之间的关系。进一步说，用户可基于与GUI窗口中另一GUI窗口的交互作用来控制（例如过滤、分类等）GUI上下文和GUI窗口显示（例如405、460、485、490等）。

[0066] 可呈现其它工具（例如495）以便于改变和控制具有屏幕截图400d的呈现。例如，可提供过滤控制495以人工过滤并指定具体安全事件子集、策略、地理位置以及控制所检测安全事件的什么子集被呈现在GUI 405、460、485、490等内或其它标准。比如，用户可指定在用户期望使用GUI 405、460、485、490等评估的安全事件集合中涉及的资产分组集合、地理、安全事件类型、管理员用户以及其它属性。进一步说，在一些示例中，用户可选择在安全事件评估中要呈现和使用的GUI类型以及两个或更多GUI同时呈现的GUI布局。更进一步说，可提供用于显示在GUI 405、460、485、490等中表示的安全事件（例如创建文件服务工具、系统告警等、未发现的安全事件）和规则的工具，除此之外还有其它示例。

[0067] 图5A和5B是阐明用于在GUI内图形表示所检测安全事件集合的地理位置属性的示例技术的简化流程图500a-b。比如，在图5A的示例中，可标识505在具体计算系统内检测的多个安全事件。在多个安全事件当中，可标识具体安全事件。可标识（例如510）安全事件所针对（例如安全事件威胁、损害、针对）的第一装置，选同包含第一装置的系统资产的具体分组。进一步说，另一装置也可被标识为至少部分负责或附属于具体安全事件的起始或源。其它标识的装置可被视为具体安全事件的源装置。进一步说，比如，可基于数据的地理位置分析或对应于源装置的标识符（诸如源装置的IP地址）。标识源装置位置，并将其与具体安全事件关联520。可生成525具体安全事件的图形表示，包含与所标识图形位置关联的源以及与所标识资产分组关联的源的表示。

[0068] 进一步说，在图5B的示例中，多个所标识（例如在505）安全事件内的安全事件的源可被检测为在所监视系统内，并针对所监视系统内的或外部的其它装置。比如，可标识530具体资产分组，其包含具体安全事件的源装置。还可标识535安全事件的一个或多个目标。这些标识的目标可被确定为在所监视系统的外部。地理位置可与外部与安全事件关联540，同时对于确定在系统内的目标可标识资产分组之一（如在图5A的示例中一样）。进一步说，可生成545具体安全事件的图形表示，包含与所标识资产分组关联的源以及与所标识图形位置关联的目标的表示。

[0069] 在图5A和/或图5B的任一示例的一些实例中，可生成GUI并使其呈现在最终用户装置上。比如，可生成适用于由最终用户装置处理以将图形表示呈现的最终用户装置上的数据。进一步说，所生成的GUI可在呈现所检测安全事件的多个图形表示。进一步说，所检测安全事件的所生成图形表示可包含所检测事件的数量、事件类型、事件严重性的图形表示，除此之外还有其它信息。在GUI和图形安全事件表示中可包含和采纳其它特征，诸如在上面比如结合图4A-4D阐明和描述的特征。进一步说，应该认识到，对于一些安全事件，对于安全事件的目标可标识地理位置，而对于安全事件的源可标识资产分组。此外，标识源装置或目标装置属于的资产分组可通过标识源装置或目标装置是所监视系统内的装置来触发。进一步说，标识对应于源装置或目标装置的地理位置可通过标识源装置或目标装置是所监视系统
外部的装置（例如第三方装置、所监视网络外部的装置、远离所监视系统的装置和子系统的装置等）来触发。

[0070] 尽管此公开已经在某些实现以及一般关联的方法方面进行了描述，但这些实现和方法的改变和替换对本领域技术人员将是显而易见的。例如，本文描述的动作可以与所述的次序不同的次序执行，并且亦获得符合需要的结果。作为一个示例，在附图中描绘的过程不一定要求所示出的具体次序或顺序次序来获得期望的结果。所阐明的系统和工具例似地采纳备选架构、组件和模块来获得类似的结果和功能性。比如，在某些实现中，多任务处理、并行处理和基于云的解决方案可能是有利的。此外，可支持各种各样的用户界面布局和功能性。其它改变在如下权利要求书的范围内。

[0071] 在此说明书中描述的主题和操作的实施例可用数字电子电路或计算机软件、固件或硬件（包含在此说明书中公开的结构以及它们的结构等效方案）或它们中的一种或多个的组合来实现。在此说明书中描述的主题的实施例被实现为一个或多个计算级程序，即编码在计算机存储介质上以便由数据处理设备执行或控制数据处理设备的计算机程序指令的一个或多个模块。备选地或除此之外，程序指令可被编码在人作为生成的传播信号上，例如机器生成的电学、光学或电磁信号，生成所述信号以对信息进行编码以便传送到适合的接收器设备以便由数据处理设备执行。计算机存储介质可以是计算机可读存储装置、计算机可读存储衬底、随机或串行存取存储器阵列或装置或者它们中的一个或多个的组合，或者包含在其中。而且，虽然计算机存储介质本质上不是传播信号，但计算机存储介质可以是编码在人为生成的传播信号中的计算机程序指令的源或目的地。计算机存储介质还可以是一个或多个单独的物理组件或介质（例如多个CD、盘或其它存储装置）（包含分布式软件环境或云计算环境），或者包含在其中。

[0072] 网络，包括核心网络和接入网（包含无线接入网），可包含一个或多个网络元素。网络元素可涵盖各种类型的路由器、交换机、网关、桥、负载均衡器、防火墙、服务器、在线服务节点、代理、处理器、模块或任何其它适合的装置、组件、元素或可操作以为在网络环境中交换信息的对象。网络元素可包含适当的处理器、存储器元件、硬件和/或软件以支持（或者否则执行）与使用处理器进行屏幕管理功能性的关联的活动。如本文所概述的。而且，网络元素可包含任何适合的组件、模块、接口或用于其操作的对象。这可包含允许数据或信息有效交换的适当算法和通信协议。

[0073] 在此说明书中描述的操作可实现为由数据处理设备对存储在一个或多个计算机可读存储装置上或从其它源接收的数据执行的操作。术语“数据处理设备”、“处理器”、“处理装置”和“计算装置”可涵盖用于处理数据的所有种类的设备、装置和机器，作为示例包含可编程处理器、计算机、片上系统或以上任中的多个或组合。设备可包含通用或专有逻辑电路，例如中央处理器单元（CPU）、刀片（blade）、专用集成电路（ASIC）或现场可编程门阵列（FPGA），除此之外还有其它适合的选项。虽然一些处理器和计算装置已经被描述和/或阐明为单个处理器，但根据所关联服务器的具体需要可使用多个处理器。对单个处理器的提及意图包含多个处理器，视情况而定。一般而言，处理器执行指令并操纵数据以执行某些操作。设备除了包含硬件之外还可包含创建正谈论的计算机程序的执行环境的代码，例如，构成处理器固件、协议栈、数据库管理系统、操作系统、交平台运行时环境、虚拟机或它们中一个或多个的组合的代码。设备以及执行环境可实现各种不同的计算模型基础设施，诸
如万维网服务、分布式计算以及网格计算基础设施。

计算机程序（也称为程序、软件、软件应用、脚本、模块、工具、（软件工具）引擎或代码）可用任何形式的编程语言编写，包含编译语言或解释语言、确定性语言或过程语言，并且它可运行任何形式部署，包含作为独立程序或作为模块、组件、子例程、对象或适合于用于在计算环境中的其它单元。例如，计算机程序可在有形介质上包含计算机可读指令、固件、连线或编程硬件或它们的任何组合，可操作以当被执行时至少执行本文所述的过程和操作。计算机程序可以，但不必，对应于文件系统中的文件。程序可被存储在持有其它程序或数据的文件部分（例如标记语言文档中存储的一个或多个脚本）中，存储在专用于正谈论的程序的单个文件中，或者存储在多个协调文件（例如存储一个或多个模块，子程序或代码部分的文件）中。计算机程序可能被部署成在一个计算机或位于一个站点或分布在多个站点并通过通信网络互连的多个计算机上执行。

程序可被实现为通过各种对象、方法或其它过程实现各种特征和功能性的各个模块，或者改为可包含若干子模块、第三方服务、组件、库等，视情况而定。相反，各种组件的特征和功能性可组合到单个组件中。视情况而定。在某些情况下，程序和软件系统可被实现为复合对象应用。例如，复合应用部分可被实现为企业Java Beans（EJB），或者设计时间组件可具有在不同平台中生成运行时间实现的能力，不同平台诸如J2EE（Java 2平台，企业版）、ABAP（高级商业应用编程）对象或Microsoft’s .NET，除此之外还有其它平台。此外，应用可表示经由网络（例如通过因特网）访问和执行的基于万维网的应用。进一步说，与具体托管应用或服务关联的一个或多个过程可被远程存储、引用或执行。例如，具体托管应用或服务的一部可以是与远程调用的应用关联的万维网服务，而托管应用的另一部分可以是为了在远程客户端而绑定的接口对象或代理。而且，任何或所有托管应用和软件服务可以是另一软件模块或企业应用（未阐明）的子应用或子模块，不脱离本公开的范围。更进一步说，托管应用的部分可由在托管应用的服务器处直接工作以及在客户端处远程工作的用户执行。

本文描述的软件应用和程序可利用一个或多个数据结构，包含数据库和数据对象。数据对象是包含可由软件函数、操作、应用、模块以及其它软件实体（诸如软件应用和服务）操作的一个或多个定义的或继承的属性和值的数据实体。在一些应用中，属性可被实现为对象元数据。进一步说，每个属性可具有定义对对象属性值的关联数据。

在本文中描述的过程和逻辑流程可由一个或多个可编程处理器执行，可编程处理器执行一个或多个计算机程序以通过给定输入数据进行操作并生成输出结果。过程和逻辑流程也可由专用逻辑电路例如FPGA（现场可编程门阵列）或ASIC（专用集成电路）执行，并且设备也可实现为专用逻辑电路。

适合于执行计算机程序的处理器作为示例包含通用和专用微处理器以及任何种类数字计算机的任何一个或多个处理器。一般而言，处理器将从只读存储器或随机存取存储器或二者接收指令和数据。计算机的必要元件是用于根据指令执行动作的处理器以及用于存储指令和数据的一个或多个存储器元件。一般而言，计算机还将包含用于存储数据的一个或多个大容量存储装置（例如磁盘、磁光盘或光盘），或操作上耦合以从其接收数据或向其传输数据，或二者。然而，计算机不是必须具有此类装置。而且，计算机可被嵌入在另一装置中，例如移动电话、个人数字助理（PDA）、平板计算机、移动音频或视频播放器、游戏控
制台、全球定位系统（GPS）接收器或便携式存储装置（例如通用串行总线（USB）闪存驱动器），这里只提到几个，适合于存储计算机程序指令和数据的装置包含所有形式非易失性存储器、介质和存储器器件，作为示例包含半导体存储器器件，例如EEPROM、EEPROM和闪存器件；磁盘，例如内部硬盘或可拆卸盘；磁光盘；以及CD-ROM和DVD-ROM盘。处理器和存储器可由专用逻辑电路补足或合并于专用逻辑电路中。

【0079】为了提供与用户的交互作用，在此说明书中描述的主题的实施例可实现在计算机上，计算机具有用于向用户显示信息的显示装置例如CRT（阴极射线管）或LCD（液晶显示器）监视器以及键盘和指点装置（例如鼠标或轨迹球），通过它们用户可向计算机提供输入。也可使用其它种类的装置来提供与用户的交互作用；例如，提供给用户的反馈可以是任何形式的感觉反馈，例如视觉反馈、听觉反馈或触觉反馈，以及来自用户的输入可以任何形式接收，包含声音输入、语音输入或触觉输入。此外，计算机可通过向装置发送文档和从装置接收文档而与用户交互作用，装置包含用户使用的远程装置。

【0080】在上述说明书中描述的主题的实施例可实现在计算机系统中，计算机系统包含后端组件（例如作为数据服务器）或包含中间件组件（例如应用服务器），或者包含前端组件（例如具有通过其用户可用在此说明书中描述的主题的实现交互作用的图形用户界面或万维网浏览器的客户端计算机），或者一个或多个此类后端、中间件或前端组件的任何组合。系统组件可通过任何形式或介质的数字数据通信（例如通信网络）互连。通信网络的示例包含可操作以允许在系统中各种计算组件之间通信的任何内部或外部网络，多个网络、子网络或它们的组合。网络组件例如传送因特网协议（IP）分组、帧中继、异步传输模式（ATM）单元、语音、视频、数据以及网络地址的其它相关信息。网络还包含一个或多个局域网（LAN）、无线网（WAN）等，例如自组对等网和/或在任何一个或多个位置的任何其它通信系统或多个系统。

【0081】计算机系统可包含客户端和服务器。客户端和服务器一般彼此远离，并且通常通过通信网络交互作用。客户端和服务器的关系凭借运行在相应计算机上并彼此具有客户端-服务器关系的计算机程序产生。在一些实施例中，服务器向客户端装置传送数据（例如HTML网页）（例如以便向与客户端装置交互作用的用户显示数据并接收来自用户的用户输入）。可在服务器从客户端装置接收在客户端装置生成的数据（例如用户交互作用的结果）。

【0082】虽然此说明书含有许多特定实现细节，但这些不被视为对任何发明的或可要求权利的范围的限制，而是作为对具体发明的具体实施例特别的特征的描述。也可在一个实施例中组合实现在此说明书中在单独实施例的上下文中描述的某些特征。相反，也可在多个实施例中单独或以任何适合的子组合来实现各个实施例的上下文中描述的各种特征。而且，尽管特征在上面可描述为以某种组合起作用，并且甚至最初像这样要求权利，但来自所要求权利的组合的一个或多个特征在一些情况下可从组合中删去，并且所要求权利的组合可被指向子组合或子组合的变形。

【0083】类似地，虽然操作在附图中按具体次序进行描绘，但这不应被理解为要求此类操作要按所出示的具体次序或按顺序次序执行，或者所有阐明的操作都要执行，以获得符合需要的结果。在某些环境下，多任务处理和并行处理可能是有利的。而且，上述描述的实施例中的各种系统组件的分离不应该被理解为在所有实施例中都需要此类分离，并且应该理解，所描述的程序组件和系统一般可一起集成在单个软件产品中或包装在多个软件产品
中。
【0084】从而，已经描述了主题的具体实施例。其它实施例在如下权利要求书的范围内。在一些情况下，在权利要求书中阐述的动作可按不同的次序执行，并且仍获得符合需要的结果。此外，在附图中描绘的过程不一定要求所示出的具体次序或顺序次序来获得符合需要的结果。
<table>
<thead>
<tr>
<th>Source</th>
<th>460</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>10.1</td>
<td></td>
</tr>
<tr>
<td>10.x</td>
<td>China</td>
<td></td>
</tr>
<tr>
<td>China</td>
<td>10.16</td>
<td>446''</td>
</tr>
<tr>
<td>Argentina</td>
<td>10.1</td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td>172.68</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td>10.1</td>
<td></td>
</tr>
</tbody>
</table>

图 4C
图 5.A

500a

505
标识多个安全事件

510
标识包含受事件中具体事件影响的目标装置的所定义的资产分组

515
标识具体事件的源装置

520
将源装置与地理位置关联

525
生成具体事件的图形表示，包含所定义的资产分组和地理位置的表示
图 5B