IBM Security QRadar SIEM
V 7.2.7

入门指南

备注

使用此信息及其支持的产品前，请阅读第 21 页的『声明』中的信息。

产品信息

本文档适用于 IBM QRadar Security Intelligence Platform V7.2.7 及后续发行版，直到被本文档的更新版本所取代。

目录

QRadar SIEM 入门简介

《IBM® Security QRadar® 入门指南》介绍了重要概念、安装过程概述以及您在用户界面中执行的基本任务。

目标读者

本资料面向负责调查和管理网络安全的安全性管理员。 要使用本指南，您必须对贵公司的网络基础结构和联网技术有所了解。

技术文档

有关如何访问更多技术文档、技术说明和发行说明的信息，请参阅访问 IBM Security 文档技术说明 (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)。

与客户支持人员联系

有关与客户支持人员联系的信息，请参阅支持与下载技术说明 (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)。

有关良好安全实践的声明

IT 系统安全性涉及通过预防、检测和应对企业内外的不当访问来保护系统和信息。不当访问可能会导致信息被篡改、销毁、盗用或滥用，并可能导致系统损坏或者被滥用，包括用于攻击他人。 没有任何 IT 系统或产品应该被认为绝对安全，并且没有任何单一产品、服务或安全措施在预防不当使用或访问方面完全有效。 IBM 的系统、产品和服务设计成合法的综合性安全途径的组成部分，这必定涉及额外的操作过程，并且可能需要其他系统、产品或服务才能实现最高效用。 IBM 不保证任何系统、产品或服务不受任何相关方的恶意或非法行为影响，也不保证能够使您的企业不受这些行为影响。

请注意:

使用本程序可能会涉及各种法律或法规，包括关于隐私、数据保护、雇佣以及电子通信和存储的法律或法规。IBM Security QRadar 只能用于合法目的并以合法方式使用。客户同意按照适用的法律、法规和政策使用本程序，并承担遵守适用的法律、法规和政策的所有责任。被许可方表示它将获取或已获取允许合法使用 IBM Security QRadar 所需的任何许可、许可权或许可证。

第 1 章 QRadar SIEM 概述

IBM Security QRadar SIEM 是一个网络安全管理平台，用于提供情境感知与合规性支持。 QRadar SIEM 将基于流的网络认知、安全事件关联以及基于资产的漏洞评估加以组合利用。

要开始使用本产品，请配置基本的 QRadar SIEM 安装、收集事件和流数据并生成报告。

日志活动

在 IBM Security QRadar SIEM 中，您可以实时地监视和显示网络事件或执行高级搜索。

日志活动选项卡以记录形式显示来自日志源（例如防火墙或路由器设备）的事件信息。使用**日志活动**选项卡以执行以下任务:

- 调查事件数据。
- 以实时方式调查发送到 QRadar SIEM 的事件日志。
- 搜索事件。
- 使用可配置的时间序列图监视日志活动。
- 识别误报以调整 QRadar SIEM。

网络活动

在 IBM Security QRadar SIEM 中，您可以调查两台主机之间的通信会话。

如果启用内容捕获选项，那么**网络活动**选项卡显示有关流量传递方式以及所传递内容的信息。通过使用**网络活动**选项卡，您可以执行下列任务:

- 以实时方式调查发送到 QRadar SIEM 的流。
- 搜索网络流。
- 使用可配置的时间序列图监视网络活动。

资产

QRadar SIEM 使用被动流数据和漏洞数据来自动创建资产概要信息，以便发现网络服务器和主机。

资产概要提供有关网络中每项已知资产（包括正在运行的服务）的信息。 资产概要信息用于关联目的，帮助减少误报。

使用**资产**选项卡以执行以下任务:

- 搜索资产。
- 查看所有已了解的资产。
- 查看已了解的资产的身份信息。
- 调整误报漏洞。

攻击

在 IBM Security QRadar SIEM 中，您可以调查攻击以确定网络问题的根本原因。

使用**攻击**选项卡可查看在网络上发生的所有攻击并完成以下任务:

- 调查网络中的攻击、源及目标 IP 地址、网络行为以及异常。
- 将来源于多个网络的事件和流与同一个目标 IP 地址相关联。
- 转至**攻击**选项卡的各个页面，以调查事件和流详细信息。
- 确定引起攻击的唯一事件。

报告

在 IBM Security QRadar SIEM 中，您可以创建定制报告或者使用缺省报告。

QRadar SIEM 提供了缺省报告模板，您可以对这些模板进行定制、更改其品牌并将其分发给 QRadar SIEM 用户。

报告模板按报告类型分组，例如合规性报告、设备报告、执行报告和网络报告。 使用**报告**选项卡可完成下列任务:

- 创建、分发和管理 QRadar SIEM 数据报告。
- 创建定制报告，以用于操作和执行。
- 将安全信息和网络信息组合为单一报告。
- 使用或编辑预先安装的报告模板。
- 使用定制徽标作为报告的品牌。 将报告分发给不同受众时，最好进行品牌标记。
- 设置生成定制报告和缺省报告的时间表。
- 以各种格式发布报告。

数据收集

QRadar SIEM 接受来自各种设备的各种格式的信息，包括安全事件、网络流量和扫描结果。

收集的数据分类为三个主要部分: 事件、流和漏洞评估 (VA) 信息。

事件数据收集

事件由防火墙、路由器、服务器以及入侵检测系统 (IDS) 或入侵防御系统 (IPS) 之类的日志源生成。

大部分日志源使用 Syslog 协议向 QRadar SIEM 发送信息。 QRadar SIEM 还支持下列协议:

- 简单网络管理协议 (SNMP)
- Java™ 数据库连接 (JDBC)
- 安全设备事件交换 (SDEE)

缺省情况下，在特定时间范围内接收到特定数目的可识别日志后，QRadar SIEM 将自动检测日志源。 成功检测到日志源后，QRadar SIEM 将向“日志源”窗口的**管理**选项卡添加相应的设备支持模块 (DSM)。

尽管大部分 DSM 包含本机日志发送功能，但某些 DSM 需要额外的配置和/或代理程序才能发送日志。配置随 DSM 类型不同而有所差异。 您必须确保 DSM 配置为采用 QRadar SIEM 支持的格式发送日志。有关配置 DSM 的更多信息，请参阅 *DSM Configuration Guide*。

某些日志源类型（例如路由器和交换机）所发送的日志不足以使 QRadar SIEM 快速检测到这些日志源并将其添加到“日志源”列表。 您可以手动添加这些日志源。 有关手动添加日志源的更多信息，请参阅 *IBM Security QRadar Log Sources User Guide*。

收集的数据分类为三个主要部分：事件、流和漏洞评估 (VA) 信息。

流数据收集

流提供有关网络流量的信息，并且可以采用各种格式（包括，Flowlog 文件、NetFlow、J-Flow、sFlow 和 Packeteer）发送到 QRadar SIEM。

通过同时接受多种流格式，QRadar SIEM 可以检测到严格依赖于事件获取信息时将会遗漏的威胁和活动。

QRadar QFlow Collector 提供对网络流量的全面应用程序检测，而不考虑应用程序在哪个端口上运行。 例如，如果因特网中继聊天 (IRC) 协议在 7500/TCP 端口上进行通信，那么 QRadar QFlow Collector 会将流量标识为 IRC，并在对话开始时捕获包。 NetFlow 和 J-Flow 仅指出端口 7500/TCP 具有流量，而未提供任何有关所使用的协议的上下文。

常用的镜像端口位置包括核心、DMZ、服务器和应用程序交换机，并且由 NetFlow 提供来自边界路由器和交换机的补充信息。

缺省情况下，QRadar QFlow Collector 处于启用状态，并且要求将镜像端口、Span 端口或分接头连接到 QRadar SIEM 设备上的可用接口。在镜像端口连接到 QRadar SIEM 设备上的任意一个网络接口时，流分析自动开始。缺省情况下，QRadar SIEM 在管理接口上监视 2055/UDP 端口上的 NetFlow 流量。有需要时，您可以分配更多 NetFlow 端口。

漏洞评估 (VA) 信息

QRadar SIEM 可以从各种第三方扫描程序导入 VA 信息。

VA 信息帮助 QRadar Risk Manager 确定活动主机、打开的端口以及潜在的漏洞。

QRadar Risk Manager 使用 VA 信息对网络中的攻击规模进行排名。

根据 VA 扫描程序类型不同，QRadar Risk Manager 可以从扫描程序服务器导入扫描结果或者以远程方式启动扫描。

QRadar SIEM 规则

规则用于对事件、流或攻击执行测试。在满足所有测试条件时，规则将生成响应。

QRadar SIEM 提供了用于检测各种活动（包括过多的防火墙拒绝、多次失败的登录尝试以及潜在的僵尸网络活动）的规则。 有关规则的更多信息，请参阅 *IBM Security QRadar Administration Guide*。

以下列表对两种规则类别进行了描述：

- 定制规则对事件、流和攻击执行测试，以检测网络中的异常活动。
- 异常检测规则对保存的流或事件搜索的结果执行测试，以检测网络中何时发生异常流量模式。

要点：具有非管理访问权的用户可以针对他们所能够访问的网络区域创建规则。 您必须具有相应的角色许可权才能管理规则。 有关用户角色许可权的更多信息，请参阅 *IBM Security QRadar Administration Guide*。

受支持的 Web 浏览器

要使 IBM Security QRadar 产品中的功能正常运行，必须使用受支持的 Web 浏览器。

访问 QRadar 系统时，系统将提示您输入用户名和密码。管理员必须先对用户名和密码进行配置。

下表列出了受支持版本的 Web 浏览器。

表 1. QRadar 产品支持的 Web 浏览器

Web 浏览器	受支持的版本
Mozilla Firefox	38.0 Extended Support Release
32 位 Microsoft Internet Explorer，启用了文档模式和浏览器模式	11.0
Google Chrome	最新版本

第 2 章 开始进行 QRadar SIEM 部署

管理员必须先部署 QRadar SIEM，然后您才能对 IBM Security QRadar SIEM 的关键功能进行评估。

要部署 QRadar SIEM，管理员必须执行下列任务:

- 安装 QRadar SIEM 设备。
- 配置 QRadar SIEM 安装。
- 收集事件、流和漏洞评估 (VA) 数据。
- 调整 QRadar SIEM 安装。

安装 QRadar SIEM 设备

管理员必须安装 QRadar SIEM 设备才能启用对用户界面的访问。

开始之前

在安装 QRadar SIEM 评估设备之前，请确保您有:

- 可以容纳双单元设备的空间。
- 机架导轨和排架（已安装）。
- 可选: 用于进行控制台访问的 USB 键盘和标准 VGA 监视器。

过程

1. 将管理网络接口连接到标注了“以太网 1”的端口。
2. 将专用电源连接插入设备背后。
3. 如果您需要进行控制台访问，请连接 USB 键盘和标准 VGA 监视器。
4. 如果设备有前面板，那么推入两侧的翼片，将该面板从设备中拔出，卸下该面板。
5. 开启设备电源。

QRadar SIEM 设备

QRadar SIEM 评估设备是双单元机架安装服务器。 此评估设备未随附机架导轨或排架。

QRadar SIEM 设备提供了 4 个网络接口。 对于此评估，请使用标注了“以太网 1”的接口作为管理接口。

您可以使用其余 3 个监视接口进行流收集。 QRadar QFlow Collector 提供了全面的网络应用程序分析，并可以在每个对话开始时执行包捕获。 流分析将在 Span 端口或分接头连接到“以太网 1”以外的任何接口时自动开始，这取决于 QRadar SIEM 设备。您可能需要执行额外的步骤才能在 QRadar SIEM 中启用 QRadar QFlow Collector 组件。

有关更多信息，请参阅 *IBM Security QRadar Administration Guide*。

限制: 对于流分析，QRadar SIEM 评估设备设定了 50 Mbps 这一限制。 请确保各个监视接口上用于流收集的总流量不超过 50 Mbps。

QRadar SIEM 配置

通过配置 QRadar SIEM，您可以查看网络层次结构并定制自动更新。

过程

1. 确保在用于访问 QRadar 产品用户界面的所有桌面系统上安装 Java 运行时环境 (JRE) V1.7 或 IBM 64-bit Runtime Environment for Java V7.0。
2. 确保使用受支持的 Web 浏览器。请参阅第 4 页的『受支持的 Web 浏览器』。
3. 如果使用 Internet Explorer，请启用文档模式和浏览器模式。
   a. 在 Internet Explorer Web 浏览器中，按 F12 以打开“开发者工具”窗口。
   b. 单击**浏览器模式**，然后选择 Web 浏览器版本。
   c. 单击**文档模式**，然后选择 **Internet Explorer 7.0 标准**。
4. 输入地址为 QRadar Console 的以下 URL 以登录到 QRadar SIEM 用户界面:

   `https://IP Address`

相关概念:

第 4 页的『受支持的 Web 浏览器』

要使 IBM Security QRadar 产品中的功能正常运行，必须使用受支持的 Web 浏览器。

网络层次结构

您可以查看按业务职能组织的不同网络区域，并根据业务价值风险划分威胁及策略信息的优先级。

QRadar SIEM 使用网络层次结构来执行下列任务:

- 了解网络流量并查看网络活动。
- 监视网络中的特定逻辑组或服务，例如市场营销、DMZ 或 VoIP。
- 监视流量，并对每个组以及组内主机的行为进行概要分析。
- 确定和标识本地及远程主机。

为了进行评估，提供了包含预定义逻辑组的缺省网络层次结构。 请复查此网络层次结构以确保其准确而完整。 如果您的环境包含未显示在预先配置的网络层次结构中的网络范围，那么必须手动添加这些范围。

网络层次结构中定义的对象在环境中不必实际存在。 所有属于基础结构的逻辑网络范围都必须定义为网络对象。

注: 如果系统未包含完整的网络层次结构，请使用**管理**选项卡来创建特定于环境的层次结构。

有关更多信息，请参阅 *IBM Security QRadar Administration Guide*。

查看网络层次结构

您可以查看网络层次结构。

过程

1. 单击**管理**选项卡。
2. 在导航窗格中，单击**系统配置**。
3. 单击**网络层次结构**图标。
4. 在**名称**列中，展开 **Regulatory_Compliance_Servers**。

   如果您的网络层次结构未包含法规一致性服务器组件，那么可以使用“邮件”组件来完成本过程的其余部分。
5. 单击嵌套的 **Regulatory_Compliance_Servers**。
6. 单击**编辑**图标。
7. 要添加合规性服务器，请遵循以下步骤:
   a. 在 **IP/CIDR** 字段中，输入合规性服务器的 IP 地址或 CIDR 范围。
   b. 单击 **(+)** 图标。
   c. 对所有合规性服务器重复上述步骤。
   d. 单击**保存**。
   e. 对任何其他要编辑的网络重复此过程。
8. 在**管理**选项卡菜单中，单击**部署更改**。

   您可以根据最新网络安全信息自动或手动更新配置文件。 QRadar SIEM 使用系统配置文件来提供网络数据流的有用特征。

自动更新

通过使用 QRadar SIEM，可以替换现有配置文件，或者将更新后的文件与现有文件集成。

QRadar SIEM 控制台必须连接到因特网才能接收更新。 如果控制台未连接到因特网，那么您必须配置内部更新服务器。有关设置自动更新服务器的信息，请参阅 *IBM Security QRadar User Guide*。

从 IBM Fix Central (www.ibm.com/support/fixcentral/) 下载软件更新。

更新文件可以包含下列更新:

- 配置更新，这包括配置文件更改、漏洞更新、QID 映射更新和安全威胁信息更新。
- DSM 更新，这包括用于更正解析问题的更新、扫描程序更改和协议更新。
- 主要更新，这包括经过更新的 JAR 文件之类的项。
- 次要更新，这包括额外的联机帮助内容或经过更新的脚本之类的项。

配置自动更新设置

您可以对 QRadar SIEM 更新频率、更新类型、服务器配置和备份设置进行定制。

过程

1. 单击**管理**选项卡。
2. 在导航窗格中，单击**系统配置**。
3. 单击**自动更新**图标。
4. 在导航窗格中，单击**更改设置**。

5. 选择**基本**选项卡。
6. 在**自动更新调度**窗格中，接受缺省参数。
7. 在**更新类型**窗格中，配置下列参数:
   a. 在**配置更新**列表框中，选中**自动更新**。
   b. 对于下列参数，接受缺省值:
      - **DSM、扫描程序和协议更新**
      - **主要更新**
      - **次要更新**
8. 取消选中**自动部署**复选框。

   缺省情况下，此复选框处于选中状态。 如果未选中此复选框，那么**仪表板**选项卡上将显示系统通知，指出安装更新后必须部署更改。
9. 单击**高级**选项卡。
10. 在**服务器配置**窗格中，接受缺省参数。
11. 在**其他设置**窗格中，接受缺省参数。
12. 单击**保存**并关闭“更新”窗口。
13. 在工具栏中，单击**部署更改**。

收集事件

通过收集事件，您可以采用实时方式对发送到 QRadar SIEM 的日志进行调查。

过程

1. 单击**管理**选项卡。
2. 在导航窗格中，单击**数据源 > 事件**。
3. 单击**日志源**图标。
4. 查看日志源列表，并对日志源进行任何必要更改。 有关配置日志源的信息，请参阅 *IBM Security QRadar Log Sources User Guide*。
5. 关闭“日志源”窗口。
6. 在**管理**选项卡菜单中，单击**部署更改**。

收集流

通过收集流，可以对主机之间的网络通信会话进行调查。

开始之前

此过程不适用于 IBM Security Intelligence on Cloud。有关如何对第三方网络设备（例如交换机和路由器）启用流的更多信息，请参阅供应商文档。

过程

1. 单击**管理**选项卡。
2. 在导航菜单中，单击**数据源 > 流**。
3. 单击**流源**图标。
4. 查看流源列表，并对流源进行任何必要更改。 有关配置流源的更多信息，请参阅 *IBM Security QRadar Administration Guide*。

5. 关闭“流源”窗口。
6. 在**管理**选项卡菜单中，单击**部署更改**。

导入漏洞评估 (VA) 信息

通过导入 VA 信息，您可以标识活动主机、打开的端口以及潜在的漏洞。

过程

1. 单击**管理**选项卡。
2. 在导航菜单中，单击**数据源 > 漏洞**。
3. 单击 **VA 扫描程序**图标。
4. 在工具栏中，单击**添加**。
5. 输入参数的值。

   参数取决于您要添加的扫描程序类型。 有关更多信息，请参阅 *Vulnerability Assessment Configuration Guide*。

   要点: “CIDR 范围”指定 QRadar SIEM 要集成到扫描结果中的网络。例如，如果要对 192.168.0.0/16 网络执行扫描并指定 192.168.1.0/24 作为 CIDR 范围，那么将仅集成 192.168.1.0/24 范围内的结果。
6. 单击**保存**。
7. 在**管理**选项卡菜单中，单击**部署更改**。
8. 单击**调度 VA 扫描程序**图标。
9. 单击**添加**。
10. 指定期望的扫描频率条件。

    根据扫描类型不同，条件包括 QRadar SIEM 导入扫描结果或启动新扫描的频率。另外，还必须指定要包括在扫描结果中的端口。
11. 单击**保存**。

QRadar SIEM 调整

您可以调整 QRadar SIEM 以满足环境需求。

在调整 QRadar SIEM 之前，请等待一天，以便启用 QRadar SIEM 来检测网络中的服务器、存储事件和流并根据现有规则创建攻击。

管理员可以执行下列调整任务:

- 通过对**日志活动**和**网络活动快速过滤**属性启用有效内容索引，优化事件和流有效内容搜索。
- 通过向构建块自动或手动添加服务器，实现更快速的初始部署并简化调整。
- 通过创建或修改定制规则及异常检测规则，配置对事件、流和攻击条件的响应。
- 确保网络中的每台主机都根据最新规则、已发现的服务器和网络层次结构来创建攻击情境。

有效内容索引编制

通过使用**日志活动**和**网络活动**选项卡上提供的**快速过滤**功能，可以搜索事件和流有效内容。

要优化**快速过滤**，可以启用有效内容索引**快速过滤**属性。

启用有效内容索引编制可能会降低系统性能。 对**快速过滤**属性启用有效内容索引编制后，监视索引统计信息。

有关索引管理和统计信息的更多信息，请参阅 *IBM Security QRadar Administration Guide*。

启用有效内容索引编制

通过对**日志活动**和**网络活动快速过滤**属性启用有效内容索引，可以优化事件和流有效内容搜索。

过程

1. 单击**管理**选项卡。
2. 在导航窗格中，单击**系统配置**。
3. 单击**索引管理**图标。
4. 在**快速搜索**字段中，输入以下项:

   快速过滤
5. 右键单击要编制索引的**快速过滤**属性。
6. 单击**启用索引**。
7. 单击**保存**。
8. 单击**确定**。
9. 可选: 要禁用有效内容索引，请选择下列其中一个选项:
   - 单击**禁用索引**。
   - 右键单击属性，然后从菜单中选择**禁用索引**。

下一步做什么

有关“索引管理”窗口中显示的参数的详细信息，请参阅 *IBM Security QRadar Administration Guide*。

服务器和构建块

QRadar SIEM 自动发现网络中的服务器并对其进行分类，从而实现更快速的初始部署并且在网络发生更改时简化调整。

为了确保对服务器类型应用适当的规则，您可以添加各个设备或者整个设备地址范围。您可以在服务器各自的“主机定义构建块”中手动输入不符合唯一协议的服务器类型。 例如，向构建块添加下列服务器类型将减少进一步调整误报的需要:

- 向 **BB:HostDefinition**: **网络管理服务器**构建块添加网络管理服务器。
- 向 **BB:HostDefinition**: **代理服务器**构建块添加代理服务器。

- 向 **BB:HostDefinition: 病毒定义和其他更新服务器**构建块添加病毒和 Windows 更新服务器。
- 向 **BB-HostDefinition: VA 扫描源 IP** 构建块添加漏洞评估 (VA) 扫描程序。

“服务器发现”功能使用资产概要信息数据库来发现网络中的多种服务器类型。 “服务器发现”功能自动列出已发现的服务器，您可以选择要包括在构建块中的服务器。

有关发现服务器的更多信息，请参阅 *IBM Security QRadar Administration Guide*。

通过使用构建块，您可以在其他规则中复用特定规则测试。 通过使用构建块调整 QRadar SIEM 并启用额外的关联规则，可以减少误报数。

将服务器自动添加到构建块

您可以将服务器自动添加到构建块。

过程

1. 单击**资产**选项卡。
2. 在导航窗格中，单击**服务器发现**。
3. 在**服务器类型**列表中，选择要发现的服务器类型。

   对于其余参数，保留缺省值不变。
4. 单击**发现服务器**。
5. 在“匹配的服务器”窗格中，选中所有要分配到服务器角色的服务器的复选框。
6. 单击**批准选定的服务器**。

   切记: 您可以右键单击任何 IP 地址或主机名以显示 DNS 解析信息。

将服务器手动添加到构建块

如果未自动检测到某台服务器，您可以将该服务器手动添加到相应的主机定义构建块。

过程

1. 单击**攻击**选项卡。
2. 在导航窗格中，单击**规则**。
3. 在**显示**列表中，选择**构建块**。
4. 在**组**列表中，选择**主机定义**。

   构建块的名称与服务器类型相对应。 例如，**BB:HostDefinition: 代理服务器**适用于环境中的所有代理服务器。
5. 要手动添加主机或网络，请双击适合于环境的相应主机定义构建块。
6. 在**构建块**字段中，单击**且当源 IP 或目标 IP 为下列其中一项时**短语后面带下划线的值。
7. 在**输入 IP 地址或 CIDR** 字段中，输入要分配给构建块的主机名或 IP 地址范围。
8. 单击**添加**。
9. 单击**提交**。
10. 单击**完成**。

11. 针对每种要添加的服务器类型重复这些步骤。

配置规则

您可以在**日志活动**、**网络活动**和**攻击**选项卡中配置规则或构建块。

过程

1. 单击**攻击**选项卡。
2. 双击要调查的攻击。
3. 单击**显示 > 规则**。
4. 双击规则。

   您可以进一步调整规则。 有关调整规则的更多信息，请参阅 *IBM Security QRadar Administration Guide*。
5. 关闭“规则”向导。
6. 在“规则”页面中，单击**操作**。
7. 可选: 如果要避免在攻击保留期过后将其从数据库中除去，请选中**保护攻击**。
8. 可选: 如果要将该攻击分配给 QRadar SIEM 用户，请选择**分配**。

清除 SIM 数据模型

清除 SIM 数据模型以确每台主机都根据最新规则、已发现的服务器和网络层次结构来创建攻击情境。

过程

1. 单击**管理**选项卡。
2. 在工具栏中，选择**高级 > 清除 SIM 模型**。
3. 选择一个选项:
   - 单击软清除，可将攻击设置为不活动。
   - 单击软清除，同时使用可选的取消激活所有的攻击复选框，可关闭所有攻击。
   - 单击硬清除，可擦除所有条目。
4. 选中**确定要重置数据模型吗?** 框。
5. 单击**继续**。
6. SIM 重置过程完成后，刷新浏览器。

结果

清除 SIM 模型时，将关闭所有的现有攻击。 清除 SIM 模型不会影响现有的事件和流。

第 3 章 开始使用 QRadar SIEM

要开始使用 IBM Security QRadar SIEM，您需要了解如何调查攻击、创建报告以及搜索事件、流和资产。

例如，可以使用**日志活动**和**网络活动**选项卡中保存的缺省搜索来搜索信息。 并且，您还可以创建并保存自己的定制搜索。

管理员可以执行下列任务:

- 使用特定条件搜索事件数据，并将满足搜索条件的事件显示在结果列表中。 对事件数据列进行选择、组织和分组。
- 以可视方式对流数据进行实时监视和调查，或者执行高级搜索以便对显示的流进行过滤。 查看流信息，以确定网络流量传递方式以及传递了何种网络流量。
- 查看所有已了解的资产，或者在环境中搜索特定资产。
- 调查网络中的攻击、源及目标 IP 地址、网络行为以及异常。
- 编辑、创建、调度和分发缺省报告或定制报告。

搜索事件

您可以搜索 QRadar SIEM 在过去 6 小时内接收到的所有认证事件。

过程

1. 单击**日志活动**选项卡。
2. 在工具栏中，选择**搜索 > 新建搜索**。
3. 在“时间范围”窗格中，定义事件搜索时间范围:
   a. 单击**最近**。
   b. 在**最近**列表中，选择**过去 6 小时**。
4. 在“搜索参数”窗格中，定义搜索参数:
   a. 在第一个列表中，选择**类别**。
   b. 在第二个列表中，选择**等于**。
   c. 在**高级别类别**列表中，选择**认证**。
   d. 在**低级别类别**列表中，接受缺省值**任何**。
   e. 单击**添加过滤器**。
5. 在“列定义”窗格中，从**显示**列表中选择**事件名称**。
6. 单击**搜索**。

相关任务:

第 18 页的『示例: 根据已保存的搜索创建定制报告』
您可以通过导入搜索或创建定制条件来创建报告。

保存事件搜索条件

您可以保存指定的事件搜索条件以供将来使用。

过程

1. 单击**日志活动**选项卡。
2. 在工具栏中，单击**保存条件**。
3. 在**搜索名称**字段中，输入**示例搜索 1**。
4. 在“时间范围选项”窗格中，单击**最近**。
5. 在**最近**列表中，选择**过去 6 小时**。
6. 单击**包括在快速搜索中**。
7. 单击**包括在仪表板中**。

   如果**包括在仪表板中**未显示，请单击**搜索 > 编辑搜索**，以验证您是否在“列定义”窗格中选择了**事件名称**。
8. 单击**确定**。

下一步做什么

配置时间序列图。 有关更多信息，请参阅『配置时间序列图』。

相关任务:

『配置时间序列图』

您可以显示交互式时间序列图，这些图表表示特定时间间隔搜索所匹配的记录。

配置时间序列图

您可以显示交互式时间序列图，这些图表表示特定时间间隔搜索所匹配的记录。

过程

1. 在图表标题栏中，单击**配置**图标。
2. 在**要绘图的值**列表中，选择**目标 IP（唯一计数）**。
3. 在**图表类型**列表中，选择**时间序列**。
4. 单击**捕获时间序列数据**。
5. 单击**保存**。
6. 单击**更新详细信息**。
7. 对搜索结果进行过滤:
   a. 右键单击要过滤的事件。
   b. 单击**基于事件名称的过滤器为 <Event Name>**。
8. 要显示按用户名分组的事件列表，请从**显示**列表中选择**用户名**。
9. 验证您的搜索是否显示在**仪表板**选项卡上:
   a. 单击**仪表板**选项卡。
   b. 单击**新建仪表板**图标。
   c. 在**名称**字段中，输入**示例定制仪表板**。
   d. 单击**确定**。
   e. 在**添加项**列表中，选择**日志活动 > 事件搜索 > 示例搜索 1**。

结果

保存的事件搜索所产生的结果将显示在仪表板中。

相关任务:

第 13 页的『保存事件搜索条件』

您可以保存指定的事件搜索条件以供将来使用。

搜索流

您可以实时地搜索、监视和调查流数据。另外，您还可以运行高级搜索，以便对显示的流进行过滤。查看流信息，以确定网络流量传递方式以及传递了何种网络流量。

过程

1. 单击**网络活动**选项卡。
2. 在工具栏中，单击**搜索 > 新建搜索**。
3. 在“时间范围”窗格中，定义流搜索时间范围:
   a. 单击**最近**。
   b. 在**最近**列表中，选择**过去 30 分钟**。
4. 在“搜索参数”窗格中，定义搜索条件。
   a. 在第一个列表中，选择**流方向**。
   b. 在第二个列表中，选择**等于**。
   c. 在第三个列表中，选择 **R2L**。
   d. 单击**添加过滤器**。
5. 在“列定义”窗格中的**显示**列表中，选择**应用程序**。
6. 单击**搜索**。

结果

这将显示过去 30 分钟内流方向为远程到本地 (R2L) 的所有流，并且这些流将按**应用程序**字段进行分组和排序。

保存流搜索条件

您可以保存指定的流搜索条件以供将来使用。

过程

1. 在**网络活动**选项卡工具栏中，单击**保存条件**。
2. 在**搜索名称**字段中，输入名称**示例搜索 2**。
3. 在**最近**列表中，选择**过去 6 小时**。
4. 单击**包括在仪表板中**和**包括在快速搜索中**。
5. 单击**确定**。

下一步做什么

创建仪表板项。 有关更多信息，请参阅第 16 页的『创建仪表板项』。

相关任务:

『创建仪表板项』
您可以使用保存的流搜索条件来创建仪表板项。

创建仪表板项

您可以使用保存的流搜索条件来创建仪表板项。

过程

1. 在**网络活动**工具栏中，选择**快速搜索 > 示例搜索 2**。
2. 验证该搜索是否包括在仪表板中:
   a. 单击**仪表板**选项卡。
   b. 在**显示仪表板**列表中，选择**示例定制仪表板**。
   c. 在**添加项**列表中，选择**流搜索 > 示例搜索 2**。
3. 配置仪表板图表:
   a. 单击**设置**图标。
   b. 通过使用配置选项，更改用于绘图的值、显示的对象数、图表类型或者图表中显示的时间范围。
4. 要调查图表中当前显示的流，请单击**在"网络活动"中查看**。

结果

"网络活动"页面将显示与时间序列图的参数相匹配的结果。 有关时间序列图表的更多信息，请参阅*IBM Security QRadar User Guide*。

相关任务:

第 15 页的『保存流搜索条件』
您可以保存指定的流搜索条件以供将来使用。

搜索资产

访问**资产**选项卡时，将显示"资产"页面，其中显示了网络中所有已发现的资产。 要优化此列表，您可以配置搜索参数，以便仅显示要调查的资产概要信息。

关于此任务

使用搜索功能可以搜索主机概要信息、资产和身份信息。 身份信息提供了更多详细信息，例如网络中的 DNS 信息、用户登录信息和 MAC 地址。

过程

1. 单击**资产**选项卡。
2. 在导航窗格中，单击**资产概要信息**。
3. 在工具栏中，单击**搜索 > 新建搜索**。
4. 如果要装入已保存的搜索，请执行下列步骤:
   a. 可选: 在**组**列表中，选择要在**可用的已保存搜索**列表中显示的资产搜索组。
   b. 选择下列其中一个选项:
      - 在**输入已保存的搜索或者从列表中进行选择**字段中，输入要装入的搜索的名称。

- 在**可用的已保存搜索**列表中，选择要装入的已保存搜索。

c. 单击**装入**。

5. 在“搜索参数”窗格中，定义搜索条件:
   a. 在第一个列表中，选择要搜索的资产参数。 例如，**主机名**、**漏洞风险分类**或**技术所有者**。
   b. 在第二个列表中，选择要用于搜索的修饰符。
   c. 在**条目**字段中，输入与搜索参数相关的特定信息。
   d. 单击**添加过滤器**。
   e. 对每个要添加到搜索条件的过滤器重复这些步骤。
6. 单击**搜索**。

示例

您将接收到一个通知，指出 CVE 标识 CVE-2010-000 正被渗透。 要确定部署中是否有任何主机容易受此渗透攻击，请执行下列步骤:

1. 从搜索参数的列表中，选择**漏洞外部引用**。
2. 选择 **CVE**。
3. 要查看易受此特定 CVE 标识攻击的所有主机的列表，请输入以下命令:

```
2010-000
```

有关更多信息，请参阅 Open Source Vulnerability Database (http://osvdb.org/) 和 National Vulnerability Database (http://nvd.nist.gov/)。

攻击调查

通过使用**攻击**选项卡，您可以调查网络中的攻击、源及目标 IP 地址、网络行为以及异常。

QRadar SIEM 可以将事件和流与同一攻击和同一网络事故中遍布多个网络的目标 IP 地址相关联。您可以有效地调查网络中的各个攻击。

查看攻击

您可以调查网络中的攻击、源及目标 IP 地址、网络行为以及异常。

过程

1. 单击**攻击**选项卡。
2. 双击要调查的攻击。
3. 在工具栏中，选择**显示 > 目标**。 您可以对各个目标进行调查，以确定该目标是否受侵害或者表现出可疑行为。
4. 在工具栏中，单击**事件**。

结果

“事件列表”窗口将显示所有与攻击相关联的事件。 您可以对事件执行搜索、排序和过滤。

示例: 启用 PCI 报告模板

通过使用**报告**选项卡，您可以启用、禁用和编辑报告模板。

关于此任务

启用支付卡行业 (PCI) 报告模板。

过程

1. 单击**报告**选项卡。
2. 取消选中**隐藏不活动报告**复选框。
3. 在**组**列表中，选择**合规性 > PCI**。
4. 选中列表中的所有报告模板:
   a. 单击列表中的第一个报告。
   b. 通过按住 Shift 键并单击列表中的最后一个报告，选中所有报告模板。
5. 在**操作**列表中，选择**切换调度**。
6. 访问所生成的报告:
   a. 从**生成的报告**列的列表中，选择要查看的报告的时间戳记。
   b. 在**格式**列中，单击要查看的报告格式的图标。

示例: 根据已保存的搜索创建定制报告

您可以通过导入搜索或创建定制条件来创建报告。

关于此任务

根据第 13 页的『搜索事件』中创建的事件搜索和流搜索来创建报告。

过程

1. 单击**报告**选项卡。
2. 在**操作**列表中，选择**创建**。
3. 单击**下一步**。
4. 配置报告计划安排。
   a. 选择**每日**选项。
   b. 选择**星期一、星期二、星期三、星期四和星期五**选项。
   c. 使用列表选择 **8:00** 和 **AM**。
   d. 确保选中**是 - 手动生成报告**选项。
   e. 单击**下一步**。
5. 配置报告布局:
   a. 在**方向**列表中，选择**横向**。
   b. 选择具有两个图表容器的布局。
   c. 单击**下一步**。
6. 在**报告标题**字段中，输入**样本报告**。
7. 配置顶部图表容器:

a. 在**图表类型**列表中，选择**事件/日志**。
b. 在**图表标题**字段中，输入**样本事件搜索**。
c. 在**事件/日志项数限制**列表中，选择 **10**。
d. 在**图形类型**列表中，选择**堆积条形图**。
e. 单击**先前的所有数据（24 小时）**。
f. 在**使此事件报告基于**列表中，选择**示例搜索 1**。

其余参数将使用已保存的搜索**示例搜索 1** 中的设置自动填写。

g. 单击**保存容器详细信息**。

8. 配置底部图表容器:
a. 在**图表类型**列表中，选择**流**。
b. 在**图表标题**字段中，输入**样本流搜索**。
c. 在**流数限制**列表中，选择 **10**。
d. 在**图形类型**列表中，选择**堆积条形图**。
e. 单击**前 24 小时的所有数据**。
f. 在**可用的已保存搜索**列表中，选择**示例搜索 2**。

其余参数将使用已保存的搜索**示例搜索 2** 中的设置自动填写。

g. 单击**保存容器详细信息**。

9. 单击**下一步**。
10. 单击**下一步**。
11. 选择报告格式:
a. 单击 **PDF 和 HTML** 复选框。
b. 单击**下一步**。
12. 选择报告分发通道:
a. 单击**报告控制台**。
b. 单击**电子邮件**。
c. 在**输入报告目标电子邮件地址**字段中，输入电子邮件地址。
d. 单击**包括报告作为附件**。
e. 单击**下一步**。
13. 填写最终的“报告”向导详细信息:
a. 在**报告描述**字段中，输入模板描述。
b. 单击**是 - 向导完成后运行此报告**。
c. 单击**完成**。
14. 使用**生成的报告**列中的列表框选择报告时间戳记。

相关任务:

第 13 页的『搜索事件』

您可以搜索 QRadar SIEM 在过去 6 小时内接收到的所有认证事件。

声明

本信息是为在美国国内供应的产品和服务而编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您所在区域当前可获得的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务的操作，由用户自行负责。

IBM 可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并不意味着授予用户使用这些专利的任何许可。 您可以用书面形式将许可查询寄往:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

有关双字节字符集 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

International Business Machines Corporation“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。 某些管辖区域在某些交易中不允许免除明示或暗含的保证。 因此本条款可能不适用于您。

此信息可能包含技术上或印刷上的错误。 将对此信息进行定期的更改；这些更改将编入该出版物的新修订版中。 IBM 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对任何非 IBM Web 站点的引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: (i) 使其能够在独立创建的程序和其它程序（包括本程序）之间进行信息交换，以及 (ii) 使其能够对已经交换的信息进行相互使用，请与下列地址联系:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本文档中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际程序许可协议或任何同等协议中的条款提供。

引用的性能数据和客户示例仅出于说明目的而提供。实际性能结果可能有所不同，这取决于特定配置和运行条件。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

所有 IBM 的价格均是 IBM 当前的建议零售价，可随时更改而不另行通知。经销商的价格可与此不同。

本信息包含日常业务运作所使用的数据和报表的示例。 为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。 所有这些名字都是虚构的，如与实际人员或商业企业有任何雷同，纯属巧合。

商标

IBM、IBM 徽标和 ibm.com® 是 International Business Machines Corp.，在全球许多管辖区域的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。Web 站点“Copyright and trademark information”(www.ibm.com/legal/copytrade.shtml) 提供了 IBM 商标的最新列表。

Java 和所有基于 Java 的商标和徽标是 Oracle 和/或其子公司的商标或注册商标。

Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

产品文档的条款和条件

根据以下条款和条件授予使用这些出版物的许可权。

适用性

除用于 IBM Web 站点的任何条款外，提供以下条款和条件。

个人用途

您可以为了个人使用而非商业性使用复制这些出版物，但前提是保留所有专有权声明。未经 IBM 的明确许可，您不得分发、显示这些出版物或其中部分出版物，也不得制作其演绎作品。

商业性用途

您仅可在贵公司内部复制、分发和显示这些出版物，但前提是保留所有专有权声明。未经 IBM 的明确许可，您不得制作这些出版物的演绎作品，也不得在贵公司外部复制、分发或显示这些出版物或其部分出版物。

权利

除非在此许可权中明确授权，否则不授予出版物或其中包含的任何信息、数据、软件或其他知识产权的任何其他许可权、许可证或权利，无论明示或暗含的。

只要 IBM 认为这些出版物的使用会损害其利益或者 IBM 判定未正确遵守上述指示信息，IBM 将有权撤销本文授予的许可权。

只有您完全遵循所有适用的法律和法规，包括所有的美国出口法律和法规，您才可以下载、出口或再出口该信息。

IBM 对这些出版物的内容不作任何保证。这些出版物“按现状”提供，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关适销、非侵权和适用于某种特定用途的保证。

IBM 网上隐私声明

IBM 软件产品，包括软件即服务解决方案（“软件产品”），可使用 cookie 或其他技术收集产品使用信息、帮助改善最终用户体验、定制与最终用户的交互或用于其他用途。在许多情况下，软件产品不收集个人可标识信息。 部分软件产品可帮助您收集个人可标识信息。 如果该软件产品使用 cookie 来收集个人可标识信息，那么有关该产品使用 cookie 的具体信息如下所述。

根据部署的配置，“软件产品” 可能使用会话 cookie 来收集每个用户的会话 ID，以用于会话管理和认证用途。 可以禁用 cookie，但是这也将删除 cookie 启用的功能。

如果为此软件产品部署的配置提供您以客户身份通过 cookie 或其他技术从最终用户收集个人可标识信息的功能，那么您应该查找关于适用于此类数据收集的所有法律的您自己的合法建议（包括声明和许可）。

有关出于这些目的使用各种技术（包括 cookie）的更多信息，请参阅 http://www.ibm.com/software/info/product-privacy 中标题为“Cookies, Web Beacons and Other

Technologies”和“IBM Software Products and Software-as-a-Service Privacy Statement”部分中的 IBM’s Privacy Policy（位于 http://www.ibm.com/privacy）和 IBM’s Online Privacy Statement（位于 http://www.ibm.com/privacy/details）。

隐私策略注意事项

IBM 软件产品，包括软件即服务解决方案（“软件产品”），可使用 cookie 或其他技术收集产品使用信息、帮助改善最终用户体验、定制与最终用户的交互或用于其他用途。在许多情况下，软件产品不收集个人可标识信息。 部分软件产品可帮助您收集个人可标识信息。 如果该软件产品使用 cookie 来收集个人可标识信息，那么有关该产品使用 cookie 的具体信息如下所述。

根据部署的配置，“软件产品” 可能使用会话 cookie 来收集每个用户的会话 ID，以用于会话管理和认证用途。 可以禁用 cookie，但是这也将删除 cookie 启用的功能。

如果为此软件产品部署的配置提供您以客户身份通过 cookie 或其他技术从最终用户收集个人可标识信息的功能，那么您应该查找关于适用于此类数据收集的所有法律的您自己的合法建议（包括声明和许可）。

有关出于这些目的使用各种技术（包括 cookie）的更多信息，请参阅 http://www.ibm.com/software/info/product-privacy 中标题为“Cookies, Web Beacons and Other Technologies”和“IBM Software Products and Software-as-a-Service Privacy Statement”部分中的 IBM’s Privacy Policy（位于 http://www.ibm.com/privacy）和 IBM’s Online Privacy Statement（位于 http://www.ibm.com/privacy/details）。

词汇表

本词汇表提供 IBM Security QRadar SIEM 软件及产品的术语和定义。

在本词汇表中，使用了下列交叉引用:

- *参见*从非首选术语引用首选术语，或者从缩写引用完整形式。
- *另见*引导您参考相关的或者对立的术语。

要了解其他术语和定义，请参阅 IBM Terminology Web 站点（在新窗口中打开）。

『(B)』 『(C)』 『(D)』 第 26 页的『(F)』 第 26 页的『(G)』 第 26 页的『(H)』 第 26 页的『(J)』 第 27 页的『(K)』 第 27 页的『(L)』 第 27 页的『(M)』 第 27 页的『(P)』 第 27 页的『(Q)』 第 27 页的『(R)』 第 28 页的『(S)』 第 28 页的『(T)』 第 28 页的『(W)』 第 28 页的『(X)』 第 28 页的『(Y)』 第 29 页的『(Z)』 第 29 页的『A』 第 29 页的『C』 第 30 页的『D』 第 30 页的『F』 第 30 页的『H』 第 30 页的『I』 第 30 页的『L』 第 30 页的『M』 第 30 页的『N』 第 30 页的『O』 第 30 页的『Q』 第 30 页的『R』 第 31 页的『S』 第 31 页的『T』 第 31 页的『W』

(B)

报告 (report)
在查询管理中，这是运行查询并对其应用某种格式而生成的格式化数据。

报告时间间隔 (report interval)
这是一个可配置的时间间隔，在此时间间隔结束时，事件处理器必须将捕获到的所有事件和流数据发送到控制台。

备用系统 (standby system)
这是在活动系统发生故障时自动进入活动状态的系统。如果启用了磁盘复制，那么此系统将从活动系统复制数据。

标准网络名称 (fully qualified network name, FQNN)
在网络层次结构中，这是包含所有部门的对象名称。下面是标准网络名称的一个示例: CompanyA.Department.Marketing。

标准域名 (fully qualified domain name, FQDN)
在因特网通信领域，这是主机系统的名称，其中包含域名的所有子名称。下面是标准域名的一个示例: rchland.vnet.ibm.com。

(C)

超流 (superflow)
这是由多个具有类似属性的流组成的单个流，旨在通过减少存储约束来增加处理能力。

重复流 (duplicate flow)
这是从不同流源接收到的同一数据传输的多个实例。

传输控制协议 (Transmission Control Protocol, TCP)
这是在因特网以及任何符合因特网工程任务组织 (IETF) 互联网络协议标准的网络中使用的通信协议。TCP 在包交换通信网络以及这类网络的互连系统中提供了可靠的主机到主机协议。另见因特网协议 (Internet Protocol)。

从本地到本地 (Local To Local, L2L)
与一个本地网络到另一本地网络的内部流量相关。

从本地到远程 (Local To Remote, L2R)
与一个本地网络到另一远程网络的内部流量相关。

从远程到本地 (Remote To Local, R2L)
这是从远程网络到本地网络的外部流量。

从远程到远程 (Remote To Remote, R2R)
这是从远程网络到另一远程网络的外部流量。

(D)

地址解析协议 (Address Resolution Protocol, ARP)
这是一种协议，用于将 IP 地址动态映射到局域网中的网络适配器地址。

动态主机配置协议 (Dynamic Host Configuration Protocol, DHCP)

这是一种通信协议，用于集中管理配置信息。例如，DHCP 向网络中的计算机自动分配 IP 地址。

端点 (endpoint)

环境中的 API 或服务的地址。API 显示一个端点并同时调用其他服务的端点。

(F)

非现场目标 (offsite target)

这是远离主站点的设备，用于接收来自事件收集器的事件或数据流。

非现场源 (offsite source)

这是远离主站点的设备，用于将规范化数据转发到事件收集器。

辅助 HA 主机 (secondary HA host)

这是连接到 HA 集群的备用计算机。主要 HA 主机发生故障时，辅助 HA 主机将承担主要 HA 主机的职责。

(G)

高可用性 (high availability, HA)

指发生节点或守护程序故障时重新配置集群系统，以便将工作负载重新分配到集群中的其余节点。

攻击 (offense)

这是作为对受监视条件的响应而发送的消息或生成的事件。例如，攻击将提供有关是否违反了某个策略或网络是否遭受攻击的信息。

管理共享 (administrative share)

对没有管理特权的用户隐藏的网络资源。管理共享为管理员提供对网络系统上的所有资源的访问权。

规模 (magnitude)

这是对特定攻击的相对重要性的度量。规模是根据相关性、严重性和可信性计算而得的加权值。

规则 (rule)

这是一组条件语句，这些语句使计算机系统能够识别关系并相应地运行自动化响应。

(H)

活动系统 (active system)

在高可用性 (HA) 集群中，这是其所有服务都处于运行状态的系统。

(J)

基于散列的消息认证代码 (Hash-Based Message Authentication Code, HMAC)

这是一种加密代码，它使用加密散列函数和密钥。

集合的引用映射 (reference map of sets)

这是将一个键映射到多个值的数据记录。例如，将特权用户列表映射到一个主机。

集群虚拟 IP 地址 (cluster virtual IP address)

这是在主要主机或辅助主机与 HA 集群之间共享的 IP 地址。

加密 (encryption)

在计算机安全性领域，这是将数据变换为某种难以理解的格式的过程，此过程使得原始数据不可获取或者只能通过解密过程获取。

简单网络管理协议 (Simple Network Management Protocol, SNMP)

这是一组协议，用于监视复杂网络中的系统和设备。有关受管设备的信息在管理信息库 (MIB) 中进行定义和存储。

结合时间间隔 (coalescing interval)

这是对事件进行捆绑的时间间隔。事件捆绑每 10 秒发生一次，并从第一个与当前结合的任何事件都不匹配的事件开始。在结合时间间隔内，前三个匹配事件将进行捆绑并发送到事件处理器。

解析顺序 (parsing order)

这是日志源定义，用户可以在其中定义共享同一个 IP 地址或主机名的日志源的重要性顺序。

局域网 (local area network, LAN)

这是一种网络，用于连接有限区域（例如单一建筑物或校园）中的多个设备，并且可以连接到更大型的网络。

(K)

开放式系统互连 (open systems interconnection, OSI)

这是符合国际标准化组织 (ISO) 信息交换标准的开放式系统互连。

开放式源代码漏洞数据库 (Open Source Vulnerability Database, OSVDB)

这是网络安全社区为网络安全社区创建的开放式源代码数据库，用于提供有关网络安全漏洞的技术信息。

可信性 (credibility)

这是介于 0 与 10 之间的数字评级，用于确定事件或攻击的完整性。随着多个源报告同一事件或攻击，可信性将增加。

客户机 (client)

这是一个软件程序或计算机，用于请求服务器提供服务。

控制台 (console)

这是一个显示站，操作员可以从中控制并观察系统操作。

(L)

累加器 (accumulator)

这是一个寄存器，可以在其中存储运算的其中一个操作数，该操作数随后将被该运算的结果替换。

流 (flow)

这是对话期间通过链路传递的单一数据传输。

流日志 (flow log)

这是流记录集合。

流源 (flow sources)

这是所捕获的流的来源。如果流来自受管主机上安装的硬件，那么将归类为内部流；如果流将发送到流收集器，那么将归类为外部流。

漏洞 (vulnerability)

操作系统、系统软件或应用程序软件组件中的安全隐患。

路由规则 (routing rule)

这是一个条件，事件数据满足此条件时，将执行条件收集和结果路由。

(M)

脉冲串 (burst)

传入事件或流的速度激增，导致超出许可的流或事件速度限制。

密钥文件 (key file)

在计算机安全性中，包含公用密钥、专用密钥、可信根和证书的文件。

(P)

凭证 (credential)

这是一组信息，用于将特定的访问权授予用户或进程。

(Q)

轻量级目录访问协议 (Lightweight Directory Access Protocol, LDAP)

这是一种开放式协议，它使用 TCP/IP 来提供对那些支持 X.500 模型的目录的访问，并且不像更为复杂的 X.500 目录访问协议 (DAP) 那样具有资源需求。例如，可以使用 LDAP 在因特网或内部网目录中查找人员、组织和其他资源。

(R)

日志源 (log source)

这是事件日志所来源于的安全设备或网络设备。

日志源扩展 (log source extension)

这是一种 XML 文件，它包含对事件有效内容中的事件进行标识和分类所需的所有正则表达式模式。

入侵防御系统 (intrusion prevention system, IPS)

这是一种系统，用于尝试拒绝潜在的恶意活动。拒绝机制可能涉及过滤、跟踪或设置速率限制。

入侵检测系统 (intrusion detection system, IDS)

这是一种软件，用于检测对网络或主机系统中的受监视资源进行的攻击尝试或成功攻击。

(S)

扫描程序 (scanner)
在 Web 应用程序中搜索软件漏洞的自动执行的安全程序。

设备支持模块 (Device Support Module, DSM)
这是一个配置文件，用于解析从多个日志源接收到的事件，并将这些事件转换为可以显示为输出的标准分类法格式。

身份 (identity)
这是来自数据源的属性集合，这些属性表示人员、组织、场所或项。

实时扫描 (live scan)
基于会话名称从扫描结果生成报告数据的漏洞扫描。

数据点 (datapoint)
这是在某个时间点计算而得的度量值。

数据库叶对象 (database leaf object)
这是数据库层次结构中的终端对象或节点。

刷新计时器 (refresh timer)
这是手动触发或者按指定时间间隔自动触发的内部设备，用于更新当前网络活动数据。

(T)

通用漏洞评分系统 (Common Vulnerability Scoring System, CVSS)
这是一个评分系统，用于对漏洞的严重性进行测量。

(W)

外部扫描装置 (external scanning appliance)
连接到网络以收集网络中资产的相关漏洞信息的机器。

网关 (gateway)
这是一种设备或程序，用于连接具有不同网络体系结构的网络或系统。

网络层 (network layer)
在 OSI 体系结构中，这是一个层，它提供用于在开放式系统与可预测服务质量之间建立路径的服务。

网络层次结构 (network hierarchy)
这是一种容器，用作网络对象的分层集合。

网络地址转换 (Network Address Translation, NAT)
在防火墙中，这是从安全因特网协议 (IP) 地址到外部注册地址的转换。这将启用与外部网络的通信，但屏蔽防火墙内侧使用的 IP 地址。

网络对象 (network object)
这是网络层次结构的一个组件。

违例 (violation)
这是绕过或违反企业策略的行为。

无类域间路由 (Classless Inter-Domain Routing, CIDR)
这是用于添加 C 类因特网协议 (IP) 地址的方法。这些地址提供给因特网服务提供商 (ISP)，以供其客户使用。CIDR 地址减小了路由表的大小，并使更多 IP 地址在组织内可用。

误报 (false positive)
这是分类为肯定（表示站点易受攻击），但用户确定实际为否定（不是漏洞，不易受攻击）的测试结果。

(X)

系统视图 (system view)
这是对构成系统的主要主机和受管主机的可视表示。

相关性 (relevance)
这是对网络中事件、类别或攻击的相对影响的测量。

协议 (protocol)
这是一组规则，用于控制通信网络中两个或两个以上设备或系统之间的通信和数据传输。

信任库文件 (truststore file)
包含可信实体的公用密钥的密钥数据库文件。

行为 (behavior)
这是操作或事件的可观察效果，包括其结果。

(Y)

严重性 (severity)
这是源对目标产生的相对威胁的测量。

叶 (leaf)
在树中，这是没有子代的条目或节点。

异常 (anomaly)
这是与网络的预期行为的偏差。

因特网服务提供商 (Internet service provider, ISP)
这是提供因特网访问的组织。

因特网控制报文协议 (Internet Control Message Protocol, ICMP)
这是一种因特网协议，网关使用此协议与源主机进行通信，例如报告数据报中的错误。

因特网协议 (Internet Protocol, IP)
这是一种协议，用于通过网络或互连网络路由数据。此协议充当较高协议层与物理网络之间的中介。另见传输控制协议 (Transmission Control Protocol)。

引用表 (reference table)
在这个表中，数据记录将已分配类型的键映射到其他键，然后将映射到的这些键映射到单一值。

引用集 (reference set)
这是网络上的事件或流派生的单一元素的列表。例如，IP 地址列表或用户名列表。

引用映射 (reference map)
这是将一个键直接映射到一个值的数据记录。例如，将一个用户名直接映射到一个全局标识。

应用程序特征符 (application signature)
这是一组唯一字符，这些字符通过检查包有效内容而获得，用于标识特定应用程序。

映射的引用映射 (reference map of maps)
这是将两个键映射到多个值的数据记录。例如，将应用程序的总字节数映射到源 IP。

有效内容数据 (payload data)
这是 IP 流中包含的除头信息和管理信息以外的应用程序数据。

域名系统 (Domain Name System, DNS)
这是一种分布式数据库系统，用于将域名映射到 IP 地址。

(Z)

侦察 (recon)
参见侦察 (reconnaissance, recon)。

侦察 (reconnaissance, recon)
收集与网络资源身份有关的信息的方法。将网络扫描和其他方法用于编译网络资源事件列表并为其分配严重性级别。

主机上下文 (host context)
这是一项服务，用于监视组件，以确保各个组件按预期方式操作。

主要 HA 主机 (primary HA host)
这是连接到 HA 集群的主计算机。

转发目标 (forwarding destination)
这是一个或多个供应商系统，用于接收来自日志源和流源的原始规范化数据。

资产 (asset)
在运营环境中已部署或将要部署的可管理对象。

子搜索 (sub-search)
这是一种功能，它允许在一组已完成的搜索结果中执行搜索查询。

子网 (subnet)
参见子网 (subnetwork)。

子网 (subnetwork, subnet)
这是划分为较小的独立子组（这些子组仍然互连）的网络。

子网掩码 (subnet mask)
对于因特网子网划分，这是一个 32 位掩码，用于标识 IP 地址的主机部分中的子网地址位。

自治系统号 (autonomous system number, ASN)
在 TCP/IP 中，这是由分配 IP 地址的中央权威机构分配给自治系统的编号。自治系统号使自动化路由算法能够区分自治系统。

A

ARP 重定向 (ARP Redirect)
这是一种 ARP 方法，用于在网络中存在问题时通知主机。

ARP 参见地址解析协议 (Address Resolution Protocol)。

ASN 参见自治系统号 (autonomous system number)。

C

CIDR 参见无类域间路由 (Classless Inter-Domain Routing)。

CVSS 参见通用漏洞评分系统 (Common Vulnerability Scoring System)。

D

DHCP 参见动态主机配置协议 (Dynamic Host Configuration Protocol)。

DNS 参见域名系统 (Domain Name System)。

DSM 参见设备支持模块 (Device Support Module)。

F

FQDN 参见标准域名 (fully qualified domain name)。

FQNN 参见标准网络名称 (fully qualified network name)。

H

HA 集群 (HA cluster)
这是一种高可用性配置，其中包含主服务器和一个辅助服务器。

HA 参见高可用性 (high availability)。

HMAC 参见基于散列的消息认证代码 (Hash-Based Message Authentication Code)。

I

ICMP 参见因特网控制报文协议 (Internet Control Message Protocol)。

IDS 参见入侵检测系统 (intrusion detection system)。

IP 多点广播 (IP multicast)
这是一种传输方式，即，将因特网协议 (IP) 数据报传输到单个多点广播组中的一组系统。

IP 参见因特网协议 (Internet Protocol)。

IPS 参见入侵防御系统 (intrusion prevention system)。

ISP 参见因特网服务提供商 (Internet service provider)。

L

L2L 参见从本地到本地 (Local To Local)。

L2R 参见从本地到远程 (Local To Remote)。

LAN 参见局域网 (local area network)。

LDAP 参见轻量级目录访问协议 (Lightweight Directory Access Protocol)。

M

Magistrate
这是一个内部组件，用于根据已定义的定制规则对网络流量和安全事件进行分析。

N

NAT 参见网络地址转换 (Network Address Translation)。

NetFlow
这是一种 Cisco 网络协议，用于监视网络流量流数据。NetFlow 数据包括客户机和服务器信息、使用的端口以及通过连接到网络的交换机和路由器流动的字节数和包数。这些数据将发送到 NetFlow 收集器，数据分析在该位置执行。

O

OSI 参见开放式系统互连 (open systems interconnection)。

OSVDB
参见开放式源代码漏洞数据库 (Open Source Vulnerability Database)。

Q

QID 映射 (QID Map)
这是一种分类法，用于标识各个唯一事件，并将事件映射到低级别和高级别类别，从而确定事件的关联方式和组织方式。

R

R2L 参见从远程到本地 (Remote To Local)。

R2R 参见从远程到远程 (Remote To Remote)。

S

SNMP 参见简单网络管理协议 (Simple Network Management Protocol)。

SOAP 这是一种基于 XML 的轻量级协议，用于在分散的分布式环境中交换信息。使用 SOAP 可以通过因特网查询和返回信息以及调用服务。

T

TCP 参见传输控制协议 (Transmission Control Protocol)。

W

Whois 服务器 (whois server)
这是一种服务器，用于检索有关已注册的因特网资源的信息，例如域名和 IP 地址分配。

索引

[C]

Printed in China