IBM Security QRadar
V 7.2.6

用户指南

说明

使用此信息及其支持的产品前，请阅读第 209 页的『声明』中的信息。

产品信息

本文档适用于 IBM QRadar Security Intelligence Platform V7.2.6 及后续发行版，直到被本文档的更新版本所取代。

目录

关于本指南

《IBM® Security QRadar® SIEM 用户指南》提供有关管理 IBM Security QRadar SIEM 的信息，其中包括“仪表板”、“攻击”、“日志活动”、“网络活动”、“资产”和“报告”选项卡。

目标读者

本指南面向所有负责调查和管理网络安全的 QRadar SIEM 用户。 本指南假定您具有 QRadar SIEM 访问权并了解贵公司的网络和联网技术。

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?uid=swg21616144)。

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:

此程序的使用可能涉及各种法律或法规，包括与隐私、数据保护、雇佣以及电子通信和存储有关的法律或法规。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 V7.2.6 中用户方面的新增功能

IBM Security QRadar V7.2.6 引入了优化的索引编制、对属性进行比较的新 CRE 测试、许可改进以及其他功能。

可以提高搜索性能的优化索引

在前发行版中，以 1 分钟为时间间隔来创建索引。现在，借助 QRadar V7.2.6 中的“超级索引”，使索引数据结构得到了优化，每小时末创建一个超级索引。尤其是对于数小时搜索，QRadar 现在以更优化的方式来扫描索引，针对破坏指标 (IOC) 类型的搜索使性能提升多达 10 倍。针对 IP 地址、域和主机名执行的搜索是 IOC 类型搜索的一些示例。QRadar 接收到的所有新数据都自动以新格式建立索引。

将仅对接收到的新数据索引进行优化。有关提高历史数据性能的更多信息，请参阅在 7.2.6 中优化 Ariel 索引技术说明 (http://www.ibm.com/support/docview.wss?uid=swg21968002)。

新的 CRE 测试

新的定制规则引擎 (CRE) 测试用于将一项属性与另一项进行比较，包括定制属性。

您选择可以将源 IP 地址与目标 IP 地址进行比较。您可以将用户名与定制属性进行比较。  了解更多...

使用 AQL WHERE 子句语法可在定制规则引擎 (CRE) 中构建复杂的比较。您可使用 AND/OR 逻辑、引用容器查找和资产模型查询。构建 WHERE 子句时，您只需输入条件。  了解更多...

许可证增强功能

QRadar V7.2.6 更改了事件影响许可证的方式。在前发行版中，由 QRadar 生成的所有事件（例如，EPS 通知、系统通知和内部生成的日志）都针对您的许可证进行计数。现在，以下内部事件不计入您的许可证:

- 系统通知
- 定制规则引擎 (CRE)
- 审计
- ADE
- 资产概要分析程序
- 来自安排的搜索的结果
- 运行状况指标
- QRadar Risk Manager 问题、模拟和内部日志记录。

只有在客户本地的设备上生成的事件才算作您的许可证用量。并且，60% 通过使用路由规则而丢弃的事件将算作贷记，最大为每秒 2000 个事件 (EPS)。

在规则和搜索结果中查看引用集

现在，您具有更多的数据访问权。以前，如果您不具有管理员特权，那么无法使用引用集信息。管理员现在可以将访问权授予您，以使您可以在搜索结果和公共规则中查看引用集。现在，可以将引用集包括在搜索和公共规则中。您可以查看引用集列表和引用集内容，并且可以导出引用集。  了解更多...

右键菜单中的“快速过滤”

现在，右键单击菜单包含针对事件和流的“快速过滤”选项。使用“快速过滤”条件可以在调查期间透视数据。您可以搜索与您的选择匹配或不匹配的项。在添加匹配/不匹配过滤器之后，右键单击菜单中将有更多搜索条件变为可用。  了解更多...

改进了查询工作流程以提供更快的数据访问速度

QRadar 改进了您与数据进行交互的方式，并且还使您能够快速展开攻击发生前后的时间。通过使用“网络活动”和“日志活动”选项卡上时间序列图表的选项，可以快速更改所显示的时间段，而不必离开活动视图。例如，如果您要调查星期二下午 4:30 在某个端点上发生的攻击，那么您可以从该攻击本身钻取至事件。您可以查看所查看时间范围前后几分钟内发生的事件，而不必打开**编辑搜索**页面。您可以指定时间段（精确到分钟），或者从下拉列表中展开时间段。  了解更多...

历史关联增强功能

IBM Security QRadar V7.2.6 引入了更好的威胁可见性，并改善了对历史关联概要文件和结果进行的管理:

经过增强的真实威胁可见性

在 IBM Security QRadar V7.2.5 中，对于任何在历史关联运行期间触发的规则，将会创建历史攻击。在 V7.2.6 中，仅当触发的规则指定必须针对检测到的事件创建攻击时，才会创建历史攻击。

经过改进的审计

每次运行或取消历史关联概要文件时，都会创建审计记录。此更改改进了监视并提高了可见性，使您能够了解哪些用户正在运行或取消历史关联运行。

新的攻击搜索功能

现在，您可以搜索根据所选历史关联概要文件创建的攻击。您还可以排除来自保存的搜索的历史关联结果。使用这些新的搜索参数，您可以将历史关联供给与实时攻击分隔开，以便进行报告。

经过改进的历史关联概要文件管理

根据您要处理的历史数据量以及指定的条件，您可能会发现关联需要很长时间才能完成。您现在可以取消正在运行的或者已排队运行的历史关联概要文件。

您可在“历史关联”窗口中排序和过滤列，以轻松找到您所要查找的信息。

查看概要文件的运行历史记录时，您可迅速了解某一次运行所创建的攻击数。只需进行一次单击，即可从历史关联目录向下钻取，以查看与概要文件条件匹配的事件或流的列表。

了解更多...

新的 AQL 字符串和统计函数

当您想要在正则表达式中查找字符串的位置或替换字符串时，请在高级搜索中使用下列 Ariel 查询语言 (AQL) 函数:

函数	描述
strpos	返回字符串在另一个字符串中的所处位置。
regex_replace	通过使用正则表达式作为搜索条件，替换字符串。
first	返回所指定列的第一个实例。
last	返回所指定列的最后一个实例。
stddev	返回样本标准差。
stddevp	返回填充标准差。

有关更多信息，请参阅 *IBM Security QRadar Ariel Query Language Guide* 中的 Supported Functions 部分。

第 2 章 关于 QRadar SIEM

QRadar SIEM 是一个网络安全管理平台，它通过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，提供了情境感知和合规性支持。

缺省许可证密钥

缺省许可证密钥提供了为期 5 周的用户界面访问权。 您登录 QRadar SIEM 后，将显示一个窗口，其中显示了临时许可证密钥的到期日期。有关安装许可证密钥的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

安全性异常和证书

如果您使用的是 Mozilla Firefox Web 浏览器，那么必须向 Mozilla Firefox 添加一个例外项才能登录 QRadar SIEM。有关更多信息，请参阅 Mozilla Firefox Web 浏览器文档。

如果您使用的是 Microsoft Internet Explorer Web 浏览器，那么访问 QRadar SIEM 系统时，将显示 Web 站点安全性证书消息。必须选择**继续浏览此网站**选项才能登录 QRadar SIEM。

浏览基于 Web 的应用程序

使用 QRadar SIEM 时，请使用 QRadar SIEM 用户界面中提供的导航选项，而不要使用 Web 浏览器的**后退**按钮。

安全情报产品中的功能

IBM Security QRadar 产品文档描述了可能仅在部分 QRadar 产品中可用的功能，例如攻击、流程、资产和历史关联。根据您所使用的产品不同，文档中记录的某些功能在您的部署中可能不可用。请复查每款产品的功能，以转到所需的信息。

IBM Security QRadar SIEM 为本地部署提供了全套安全情报功能。QRadar SIEM 将合并来自分布于整个网络中的设备端点和应用程序的日志源事件数据，并对原始数据执行立即的规范化和关联活动，以区分真实威胁与误报。

使用 IBM Security Intelligence on Cloud 可在托管环境中收集、分析、归档和存储大量的网络及安全事件日志。分析数据以深入了解发展中的威胁，并满足合规性监视和报告需求，同时降低总拥有成本。

使用 IBM Security QRadar Log Manager 可收集、分析、归档和存储大量的网络及安全事件日志。QRadar Log Manager 将分析数据以深入了解发展中的威胁，并可帮助您满足合规性监视和报告需求。

当您寻求帮助时，请使用下表，其中列出了产品的功能:

表 1. QRadar 功能的比较

功能	QRadar SIEM	IBM Security Intelligence on Cloud	IBM Security QRadar Log Manager
支持托管部署	否	是	否
可定制的仪表板	是	是	是
定制规则引擎	是	是	是
管理网络和安全事件	是	是	是
管理主机和应用程序日志	是	是	是
基于阈值的警报	是	是	是
合规性模板	是	是	是
数据归档	是	是	是
IBM Security X-Force® Threat Intelligence IP 声誉订阅源集成	是	是	是
WinCollect 独立部署	是	是	是
WinCollect 受管部署	是	否	是
QRadar Vulnerability Manager 集成	是	否	是
网络活动监视	是	否	否
资产概要分析	是	是	否 [1]
攻击管理	是	是	否
网络流捕获与分析	是	否	否
历史关联	是	是	否
QRadar Risk Manager 集成	是	否	否
QRadar Incident Forensics 集成	是	否	否

[1] 只有在安装了 QRadar Vulnerability Manager 时，QRadar Log Manager 才会跟踪资产数据。

支持 Web 浏览器

为了使 IBM Security QRadar 产品中的功能正常工作，必须使用支持的 Web 浏览器。

访问 QRadar 系统时，会提示您输入用户名和密码。 用户名和密码必须由管理员提前配置。

下表列出了受支持的 Web 浏览器版本。

表 2. 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（已启用文档模式和浏览器模式）。	10.0
32 位和 64 位 Microsoft Internet Explorer，以文档模式选中 Microsoft Internet Explorer 10。	11.0

表 2. QRadar 产品支持的 Web 浏览器 (续)

Web 浏览器	受支持的版本
Google Chrome	V46

在 Internet Explorer 中启用文档模式和浏览器模式

如果使用 Microsoft Internet Explorer 来访问 IBM Security QRadar 产品，则必须启用浏览器模式和文档模式。

过程

1. 在 Internet Explorer Web 浏览器中，按 F12 以打开“开发者工具”窗口。
2. 单击**浏览器模式**，然后选择 Web 浏览器版本。
3. 单击**文档模式**，然后选择对应于您的 Internet Explorer 发行版的 **Internet Explorer 标准**。

IBM Security QRadar 登录

IBM Security QRadar 是基于 Web 的应用程序。QRadar 使用 URL、用户名和密码的缺省登录信息。

登录 IBM Security QRadar 控制台时，请使用下表中的信息。

表 3. QRadar 的缺省登录信息

登录信息	缺省值
URL	https://<IP Address>，其中 <IP Address> 是 QRadar 控制台的 IP 地址。 要在 IPv6 或混合环境中登录 QRadar，请用方括号将 IP 地址括起: `https://[<IP Address>]`
用户名	admin
密码	安装期间分配给 QRadar 的密码。
许可证密钥	缺省许可证密钥，授予您对系统为期 5 周的访问权。

RESTful API

使用具象状态传输 (REST) 应用程序编程接口 (API) 可以执行 HTTPS 查询并使用其他解决方案来调查 IBM Security QRadar。

访问权和用户角色许可权

您必须在 QRadar 中具有管理用户角色许可权才能访问和使用 RESTful API。 有关如何管理用户角色许可权的更多信息，请参阅 *Administration Guide*。

访问 REST API 技术文档用户界面

API 用户界面提供以下 REST API 接口的描述和功能:

表 4. REST API 接口

REST API	描述
/api/ariel	查询数据库、搜索、搜索标识和搜索结果。
/api/asset_model	返回包含模型中所有资产的列表。 您还可以列出所有可用的资产属性类型和已保存的搜索，以及更新资产。
/api/auth	注销并使当前会话失效。
/api/help	返回 API 能力列表。
/api/siem	返回包含所有攻击的列表。
/api/qvm	查看和管理 QRadar Vulnerability Manager 数据。
/api/reference_data	查看和管理参考数据集合。
/api/qvm	检索资产、漏洞、网络、开放服务、网络及过滤器。 您还可以创建或更新补救凭单。
/api/scanner	查看、创建或启动与扫描概要文件有关的远程扫描。

REST API 技术文档接口提供了您可用于收集所需代码的框架，您需要使用此代码将 QRadar 功能实施到其他产品中。

1. 在浏览器中输入下列 URL 以访问技术文档接口: https://*ConsoleIPaddress*/api_doc。
2. 单击您要访问的 API 的头，例如 **/ariel**。
3. 单击您要访问的端点的子头，例如 **/databases**。
4. 单击 Experimental 或 Provisional 子头。

   注:

   API 端点将注释为 *experimental* 或 *stable*。

   Experimental

   指示可能未全面测试 API 端点并且可能会在以后更改或除去该 API 端点而不另行通知。

   稳定 指示全面测试并支持 API 端点。
5. 单击**尝试**以接收格式设置正确的 HTTPS 响应。
6. 查看并收集需要在第三方解决方案中实施的信息。

QRadar API 论坛和代码样本

API 论坛提供了有关 REST API 的更多信息，包括常见问题的答案以及您可以在测试环境中使用的已注释代码样本。 有关更多信息，请参阅 API 论坛 (https://www.ibm.com/developerworks/community/forums/html/forum?id=b02461a3-9a70-4d73-94e8-c096abe263ca)。

用户界面选项卡

功能以选项卡形式进行划分。 登录后，系统将显示**仪表板**选项卡。

您可以轻松浏览选项卡，以找到所需的数据或功能。

“仪表板”选项卡

仪表板选项卡是您登录后显示的缺省选项卡。

仪表板选项卡提供了支持多个仪表板的工作空间环境，在这些仪表板上可以显示 QRadar 所收集的网络安全、活动或数据的视图。共有 5 个可用的缺省仪表板。每个仪表板都包含多个项，用于提供关于网络中发生的攻击的摘要和详细信息。您还可以创建定制仪表板，以便将注意力集中到安全或网络操作职责方面。有关使用“仪表板”选项卡的更多信息，请参阅仪表板管理。

“攻击”选项卡

攻击选项卡将使您能够查看网络中发生的攻击，您可以使用各个导航选项或通过强大的搜索来查找这些攻击。

从**攻击**选项卡中，可以调查攻击以确定问题的根本原因。您还可以解决问题。

有关**攻击**选项卡的更多信息，请参阅攻击管理。

“日志活动”选项卡

日志活动选项卡使您能够以实时方式对正发送到 QRadar 的事件日志进行调查，执行强大的搜索以及使用可配置的时间序列图表查看日志活动。

日志活动选项卡允许您对事件数据执行深入调查。

有关更多信息，请参阅日志活动调查。

“网络活动”选项卡

使用**网络活动**选项卡可对实时发送的流进行调查、执行强大的搜索以及通过可配置的时间序列图表查看网络活动。

流是两个主机之间的通信会话。 查看流信息使您能够确定流量的传送方式、传送的内容（如果启用了内容捕获选项）以及执行传送的人员。另外，流数据还包含协议、ASN 值、IFIndex 值和优先级之类的详细信息。

有关更多信息，请参阅网络活动调查。

“资产”选项卡

QRadar 自动发现网络中运行的资产、服务器和主机。

自动发现以被动流数据和漏洞数据为基础，允许 QRadar 构建资产概要文件。

资产概要文件提供有关网络中每项已知资产的信息，包括身份信息（如果有）以及正在对每项资产运行哪些服务。此概要文件数据用于进行关联，以帮助减少误报。

例如，某个攻击尝试使用对特定资产运行的特定服务。在这种情况下，QRadar 可以通过使此攻击与资产概要文件相关联来确定该资产是否易受此攻击伤害。通过使用**资产**选项卡，您可以查看已了解的资产，或者搜索特定资产以查看其概要文件。

有关更多信息，请参阅资产管理。

“报告”选项卡

通过**报告**选项卡，您可以针对 QRadar 中的任何数据创建、分发和管理报告。

通过“报告”功能部件，您可以创建定制报告以供操作和执行使用。 要创建报告，可以将信息（例如，安全或网络）组合到单个报告中。 您也可以使用 QRadar 随附的预安装的报告模板。

另外，**报告**选项卡还使您能够通过定制徽标标记报告。 将报告分发给其他读者时，此定制十分有益。

有关报告的更多信息，请参阅报告管理。

IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager 是一个单独安装的设备，用于监视设备配置，模拟对网络环境的更改，以及对网络中的风险和漏洞划分优先级。

IBM Security QRadar Risk Manager 使用配置数据从网络和安全设备（例如防火墙、路由器、交换机或 IPS）、漏洞订阅源以及供应商安全源所收集的数据。 此数据用于确定网络安全基础结构内的安全、策略及合规性风险，以及这些风险被利用的几率。

注: 有关 IBM Security QRadar Risk Manager 的更多信息，请与本地销售代表联系。

“管理”选项卡

管理员可以使用“管理”选项卡来配置和管理用户、系统、网络、插件及组件。具有管理特权的用户可以访问**管理**选项卡。

表 1 对管理员在**管理**选项卡中可以访问的管理工具进行了描述。

表 5. QRadar 中提供的管理工具

管理工具	描述
系统配置	配置系统和用户管理选项。
数据源	配置日志源、流源和漏洞选项。
远程网络和服务配置	配置远程网络和服务组。
部署编辑器	管理 QRadar 部署的各个组件。

您在**管理**选项卡中进行的所有配置更新都将保存到暂存区域。完成所有更改后，您可以将这些配置更新部署到部署中的受管主机。

QRadar 通用过程

QRadar 用户界面上的多种控件对于大多数用户界面选项卡是通用的。

下列各节说明了有关这些通用过程的信息。

查看消息

位于用户界面右上角的**消息**菜单提供了对某个窗口的访问权，您可以在此窗口中阅读和管理系统通知。

开始之前

要使系统通知显示在**消息**窗口中，管理员必须根据每种通知消息类型创建一个规则，并在**定制规则向导**中选中**通知**复选框。

关于此任务

消息菜单指示系统中包含的未读系统通知数。 在您关闭系统通知之前，此指标数字将递增。 对于每个系统通知，**消息**窗口都提供了摘要以及有关系统通知创建日期的日期戳。可以将鼠标指针悬停在通知上方来查看更多详细信息。 通过使用**消息**窗口中的功能，您可以管理系统通知。

另外，**仪表板**选项卡以及一个可选弹出窗口中也提供了系统通知，此窗口可以显示在用户界面的左下角。 在**消息**窗口中执行的操作将传播到**仪表板**选项卡以及此弹出窗口。例如，如果在**消息**窗口中关闭了某个系统通知，那么此系统通知将从所有系统通知显示中除去。

有关仪表板系统通知的更多信息，请参阅系统通知项。

消息窗口提供了下列功能:

表 6. “消息”窗口中提供的功能

功能	描述
全部	单击**全部**以查看所有系统通知。 此选项是缺省选项，因此，仅当您选择了另一选项并且希望重新显示所有系统通知时，才需要单击**全部**。
运行状况	单击**运行状况**可以仅查看严重性级别为“运行状况”的系统通知。
错误	单击**错误**可以仅查看严重性级别为“错误”的系统通知。
警告	单击**警告**可以仅查看严重性级别为“警告”的系统通知。
参考	单击**参考**可以仅查看严重性级别为“参考”的系统通知。
隐藏全部	单击**隐藏全部**可以关闭系统中的所有系统通知。 如果您使用**运行状况**、**错误**、**警告**或**参考**图标对系统通知列表进行了过滤，那么**查看全部**图标将更改为下列其中一个选项: • **隐藏所有错误** • **隐藏全部运行状况** • **隐藏所有警告** • **隐藏所有警告** • **隐藏所有参考**

表 6. “消息”窗口中提供的功能 (续)

功能	描述
查看全部	单击**查看全部**可以查看**日志活动**选项卡中的系统通知事件。如果您使用**运行状况**、**错误**、**警告**或**参考**图标对系统通知列表进行了过滤，那么**查看全部**图标将更改为下列其中一个选项: • **查看所有错误** • **查看全部运行状况** • **查看所有警告** • **查看所有参考**
隐藏	单击系统通知旁边的**隐藏**图标可以在系统中关闭系统通知。

过程

1. 登录 QRadar。
2. 在用户界面的右上角，单击**消息**。
3. 在**消息**窗口中，查看系统通知详细信息。
4. 可选。 要优化系统通知列表，请单击下列其中一个选项:
   - **错误**
   - **警告**
   - **参考**
5. 可选。 要关闭系统通知，请选择下列其中一个选项:

选项	描述
隐藏全部	单击此选项可以关闭所有系统通知。
隐藏	单击要关闭的系统通知旁边的**隐藏**图标。

6. 可选。 要查看系统通知详细信息，请将鼠标指针悬停在此系统通知上方。

对结果进行排序

通过单击列标题，可以对表中的结果进行排序。列顶部的箭头指示排序方向。

过程

1. 登录 QRadar。
2. 单击列标题一次，以便按降序顺序排列表；单击列标题两次，以便按升序顺序排列表。

刷新和暂停用户界面

您可以手动刷新、暂停和播放选项卡上显示的数据。

关于此任务

仪表板和**攻击**选项卡每 60 秒自动刷新一次。

如果您是以“上次时间间隔（自动刷新）”方式查看**日志活动**和**网络活动**选项卡，那么这些选项卡将每 60 秒自动刷新一次。

界面右上角的计时器指示距离选项卡自动刷新的时间长度。

以“实时（流式方法）”或“上一分钟（自动刷新）”方式查看**日志活动**或**网络活动**选项卡时，可以使用**暂停**图标来暂停当前显示。

另外，还可以暂停**仪表板**选项卡中的当前显示。 在仪表板项内的任意位置单击将自动暂停该选项卡。 计时器将以红色闪烁，以指示当前显示已暂停。

过程

1. 登录 QRadar。
2. 单击要查看的选项卡。
3. 选择下列其中一个选项:

选项	描述
刷新	单击选项卡右上角的**刷新**可以刷新该选项卡。
暂停	单击此选项可以暂停选项卡上的显示。
播放	单击此选项可以在计时器暂停后重新启动计时器。

调查 IP 地址

您可以使用多种方法调查有关“仪表板”、“日志活动”和“网络活动”选项卡上的 IP 地址的信息。

过程

1. 登录 QRadar。
2. 单击要查看的选项卡。
3. 将鼠标指针移动到 IP 地址上，以查看其位置。
4. 右键单击 IP 地址或资产名称，然后选择下列其中一个选项:

表 7. IP 地址信息

选项	描述
浏览 > 按网络查看	显示与所选 IP 地址相关联的网络。
浏览 > 查看源摘要	显示与所选源 IP 地址相关联的攻击。
浏览 > 查看目标摘要	显示与所选目标 IP 地址相关联的攻击。
信息 > DNS 查找	根据 IP 地址搜索 DNS 条目。
信息 > WHOIS 查找	搜索远程 IP 地址的已注册所有者。 缺省 WHOIS 服务器为 whois.arin.net。
信息 > 端口扫描	对所选 IP 地址执行网络映射器 (NMAP) 扫描。 仅当系统上安装了 NMAP 时，此选项才可用。 有关安装 NMAP 的更多信息，请参阅供应商文档。

表 7. IP 地址信息 (续)

选项	描述
信息 > 资产概要文件	显示资产概要信息。 购买 IBM Security QRadar Vulnerability Manager 并获得此产品的使用授权后，将显示此选项。 有关更多信息，请参阅 *IBM Security QRadar Vulnerability Manager User Guide*。 如果 QRadar 通过扫描主动获取了概要文件数据，或者通过流源被动地获取了此数据，那么此菜单选项可用。 有关信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
信息 > 搜索事件	搜索与此 IP 地址相关联的事件。
信息 > 搜索流	搜索与此 IP 地址相关联的流。
信息 > 搜索连接	搜索与此 IP 地址相关联的连接。 仅当您购买了 IBM Security QRadar Risk Manager 并将 QRadar 与 IBM Security QRadar Risk Manager 设备连接后，才会显示此选项。有关更多信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。
信息 > 交换机端口查找	确定 Cisco IOS 设备上此 IP 地址的交换机端口。 此选项仅适用于使用**风险**选项卡上的**发现设备**选项发现的交换机。 **注**: 此菜单选项在 QRadar Log Manager 中不可用
信息 > 查看拓扑	显示**风险**选项卡，此选项卡对网络的第 3 层拓扑进行了描述。 仅当您购买了 IBM Security QRadar Risk Manager 并将 QRadar 与 IBM Security QRadar Risk Manager 设备连接后，此选项才可用。
运行漏洞扫描	选择**运行漏洞扫描**选项将对此 IP 地址运行 IBM Security QRadar Vulnerability Manager 扫描。 仅当您购买了 IBM Security QRadar Vulnerability Manager 并获得此产品的使用授权后，才会显示此选项。 有关更多信息，请参阅 *IBM Security QRadar Vulnerability Manager User Guide*。

调查用户名

您可以右键单击用户名以访问更多菜单选项。使用这些选项可以查看更多关于用户名或 IP 地址的信息。

购买 IBM Security QRadar Vulnerability Manager 并获得此产品的使用授权后，您可以对用户名进行调查。 有关更多信息，请参阅 *IBM Security QRadar Vulnerability Manager User Guide*。

右键单击用户名后，可以选择下列菜单选项。

表 8. 用于进行用户名调查的菜单选项

选项	描述
查看资产	显示与所选用户名关联的当前资产。有关查看资产的更多信息，请参阅资产管理。
查看用户历史记录	显示过去 24 小时内与所选用户名关联的所有资产。
查看事件	显示与所选用户名关联的事件。 有关“事件列表”窗口的更多信息，请参阅日志活动监视。

有关定制右键单击菜单的更多信息，请参阅产品的 *Administration Guide*。

系统时间

QRadar 用户界面的右下角显示了系统时间，此时间就是控制台上的时间。

控制台时间用于对 QRadar 部署中的 QRadar 系统进行同步。控制台时间用于确定从其他设备接收到事件的时间，以便进行正确的时间同步关联。

在分布式部署中，控制台与您的台式计算机可能处于不同的时区。

在**日志活动** 和**网络活动**选项卡中，您必须使用控制台系统时间来指定时间范围。

在**日志活动**选项卡上应用基于时间的过滤器及搜索时，您必须使用控制台系统时间来指定时间范围。

更新用户首选项

在主要 IBM Security QRadar SIEM 用户界面中，您可以设置用户首选项，例如，语言环境。

过程

1. 要访问用户信息，请单击**首选项**。
2. 更新首选项。

选项	描述
用户名	显示用户名。 不能编辑此字段。
密码	QRadar 用户密码存储为加密盐 SHA-256 字符串。 密码必须满足以下条件: • 最少包含 6 个字符 • 不能超过 255 个字符 • 至少包含 1 个特殊字符 • 包含 1 个大写字符
密码（确认）	密码确认

选项	描述
电子邮件地址	电子邮件地址必须满足以下要求: • 最少包含 10 个字符 • 不能超过 255 个字符
语言环境	QRadar 提供下列语言版本: 英语、简体中文、繁体中文、日语、韩国语、法语、德语、意大利语、西班牙语、俄语和葡萄牙语（巴西）。 如果选择其他语言，用户界面将显示英语。 使用其他相关的文化约定，例如，字符类型、整理规则、日期和时间格式、货币单位。
启用弹出通知	如果希望用户界面上显示弹出系统通知，请选中此复选框。

相关概念:

第 138 页的『快速过滤搜索选项』
通过输入使用简单单词或短语的文本搜索字符串来搜索事件和流有效内容。

访问联机帮助

通过 QRadar 主用户界面可以访问 QRadar 联机帮助。

要访问联机帮助，请单击**帮助 > 帮助内容**。

调整列的大小

您可以调整 QRadar 中某些选项卡上的列的大小。

将鼠标指针悬停在列分隔线上方，然后将列的边缘拖动到新位置。 另外，您也可以双击列分隔线，以便将列的大小自动调整为最大字段的宽度。

注: 在 Microsoft Internet Explorer V7.0 Web 浏览器中，当选项卡以流方式显示记录时无法调整列大小。

页面大小

具有管理特权的用户可以配置在 QRadar 各个选项卡上的表中显示的最大结果数。

第 3 章 仪表板管理

仪表板选项卡是您登录后显示的缺省视图。

此选项卡提供了支持多个仪表板的工作空间环境，在这些仪表板上可以显示所收集的网络安全、活动或数据的视图。

通过使用仪表板，您可以将仪表板项组织为功能性视图，从而使您能够将注意力集中到特定网络区域。

使用“仪表板”选项卡可以监视安全事件行为。

您可以对仪表板进行定制。**仪表板**选项卡中显示的内容特定于用户。在会话中进行的更改仅影响您的系统。

缺省仪表板

使用缺省仪表板对各个项进行定制，将其引入功能视图。 这些功能视图侧重于特定网络区域。

仪表板选项卡提供了 5 种缺省仪表板，这些仪表板侧重于安全性、网络活动应用程序活动、系统监视和合规性。

每个仪表板都显示了一组缺省的仪表板项。仪表板项用作浏览到更详细数据的起点。 下表定义了缺省仪表板。

定制仪表板

您可以对仪表板进行定制。**仪表板**选项卡中显示的内容特定于用户。在 QRadar 会话中进行的更改仅影响您的系统。

要定制**仪表板**选项卡，您可以执行下列任务:

- 创建与您的职责有关的定制仪表板。每个用户的最大仪表板数目为 255；但是，如果创建 10 个以上仪表板，那么可能会出现性能问题。
- 对缺省仪表板或定制仪表板添加和除去仪表板项。
- 移动和安排各个项的位置，以满足您的需求。放置项时，各个项将按相对于仪表板的比例自动调整大小。
- 添加基于任何数据的定制仪表板项。

例如，您可以添加一个仪表板项，用于提供表示排名前 10 位的网络活动的时间序列图或条形图。

要创建定制项，您可以在**网络活动**或**日志活动**选项卡上创建保存的搜索，并选择结果在仪表板中的表示方式。每个仪表板图表都显示实时的最新数据。仪表板上的时间序列图每 5 分钟刷新一次。

定制仪表板

您可以向缺省仪表板或定制仪表板添加多个仪表板项。

您可以对仪表板进行定制，以使其显示并组织满足网络安全需求的仪表板项。

共有 5 个缺省仪表板，您可以从**仪表板**选项卡上的**显示仪表板**列表框中访问这些仪表板。如果您之前查看了某个仪表板，然后返回到**仪表板**选项卡，那么将显示您最后查看的仪表板。

流搜索

在**网络活动**选项卡中可以根据已保存的搜索条件显示定制仪表板项。

流搜索项在**添加项** > **网络活动** > **流搜索**菜单中列出。 流搜索项的名称与该项所基于的已保存搜索条件的名称相匹配。

提供了缺省的已保存搜索条件，此条件预先配置为在**仪表板**选项卡菜单中显示流搜索项。 您可以向**仪表板**选项卡菜单添加更多流搜索仪表板项。 有关更多信息，请参阅向“添加项”列表添加基于搜索的仪表板项。

在流搜索仪表板项中，搜索结果将在图表中显示最新实时数据。支持的图表类型包括时间序列图、表、饼图和条形图。缺省图表类型为条形图。这些图表均可配置。有关配置图表的更多信息，请参阅配置图表。

时间序列图表是交互式图表。通过使用时间序列图表，您可以通过放大并快速扫描时间线来调查网络活动。

攻击

您可以向仪表板添加一些与攻击有关的项。

注: 隐藏或关闭的攻击不包含在**仪表板**选项卡中显示的值中。有关隐藏或关闭的事件的更多信息，请参阅攻击管理。

下表对攻击项进行了描述:

表 9. 攻击项

仪表板项	描述
最近的攻击	标识最近 5 个攻击，以规模条指示攻击严重性。将鼠标指针指向攻击名称可查看 IP 地址的详细信息。
最严重的攻击	标识 5 个最严重的攻击，以规模条指示攻击严重性。将鼠标指针指向攻击名称可查看 IP 地址的详细信息。
我的攻击	**我的攻击**项显示最近分配给您的 5 个攻击。这些攻击由规模条标识以指示攻击严重性。将鼠标指针指向 IP 地址可查看 IP 地址的详细信息。

表 9. 攻击项 (续)

仪表板项	描述
排名靠前的来源	**排名靠前的来源**项显示排名靠前的攻击源。每个来源由规模条标识以指示来源严重性。将鼠标指针指向 IP 地址可查看 IP 地址的详细信息。
排名靠前的本地目标	**排名靠前的本地目标**项显示排名靠前的本地目标。每个目标由规模条标识以指示目标严重性。将鼠标指针指向 IP 地址可查看 IP 的详细信息。
类别	**排名靠前的类别类型**项显示与最大攻击数关联的前 5 个类别。

日志活动

日志活动仪表板项允许您以实时方式监视和调查事件。

注: 隐藏或关闭的事件不包含在**仪表板**选项卡中显示的值中。

表 10. 日志活动项

仪表板项	描述
事件搜索	在“日志活动”选项卡中可以根据已保存的搜索条件显示定制仪表板项。事件搜索项在**添加项** > **网络活动** > **事件搜索**菜单中列出。事件搜索项的名称与该项所基于的已保存搜索条件的名称相匹配。 QRadar 包含缺省的已保存搜索条件，此条件预先配置为在**仪表板**选项卡菜单中显示事件搜索项。您可以向**仪表板**选项卡菜单添加更多事件搜索仪表板项。有关更多信息，请参阅『向“添加项”列表添加基于搜索的仪表板项』。 在**日志活动**仪表板项中，搜索结果将在图表中显示实时的最新数据。支持的图表类型包括时间序列图、表、饼图和条形图。缺省图表类型为条形图。这些图表均可配置。 时间序列图表是交互式图表。您可以通过放大并快速扫描时间线来调查日志活动。
事件（按严重性排列）	**事件（按严重性排列）**仪表板项显示按严重性分组的活动事件数。该项允许您按指定的严重性级别查看所接收的事件数。严重性指示攻击源所产生的威胁相对于目标应对攻击的准备情况的严重程度。严重性范围为 0（低）到 10（高）。支持的图表类型包括表、饼图和条形图。

表 10. 日志活动项 (续)

仪表板项	描述
排名靠前的日志源	**排名靠前的日志源**仪表板项显示过去 5 分钟内向 QRadar 发送事件数排名前 5 位的日志源。 饼图中指示了从指定日志源发送的事件数。该项允许您查看潜在的行为变化，例如，如果通常未包括在排名前 10 位列表中的防火墙日志源现在占了整体消息计数的较大百分比，那么您应该对此情况进行调查。支持的图表类型包括表、饼图和条形图。

最近的报告

最近的报告仪表板项显示最近生成的报告。

显示的内容提供了报告标题、报告生成日期和时间以及报告格式。

系统摘要

系统摘要仪表板项提供过去 24 小时内的活动的高级别摘要。

在摘要项中，可以查看以下信息:

- **当前每秒流量** - 显示每秒的流速率。
- **流数（过去 24 小时）** - 显示过去 24 小时内遇到的活动流的总数。
- **当前每秒事件数** - 显示每秒的事件速率。
- **新事件数（过去 24 小时）** - 显示过去 24 小时内接收到的新事件的总数。
- **更新的攻击数（过去 24 小时）** - 显示过去 24 小时内使用新证据创建或修改的攻击总数。
- **数据减少比例** - 根据过去 24 小时内检测到的事件总数以及过去 24 小时内进行了修改的攻击数，显示减少的数据所占的比例。

风险监视仪表板

您可以使用**风险监视**仪表板来监视资产、策略和策略组的策略风险及策略风险更改。

缺省情况下，**风险监视**仪表板显示**风险**和**风险更改**项，这些项监视高脆弱性、中的脆弱性和低脆弱性策略组中资产的策略风险分数以及 CIS 策略组中策略风险分数的合规性传递速率和历史更改。

风险监视仪表板项不会显示任何结果，除非您获得了 IBM Security QRadar Risk Manager 的使用授权。有关更多信息，请参阅《QRadar Risk Manager 用户指南》。

要查看缺省的**风险监视**仪表板，请在**仪表板**选项卡上选择**显示仪表板 > 风险监视**。

相关任务:

第 21 页的『监视策略合规性』

创建用于显示所选资产、策略和策略组的策略合规性传递速率和策略风险分数的仪表板项。

第 22 页的『监视风险更改』
创建用于显示所选资产、策略和策略组的每天、每周和每月的策略风险更改的仪表板项。

监视策略合规性

创建用于显示所选资产、策略和策略组的策略合规性传递速率和策略风险分数的仪表板项。

过程

1. 单击**仪表板**选项卡。
2. 在工具栏上，单击**新建仪表板**。
3. 输入策略合规性仪表板的名称和描述。
4. 单击**确定**。
5. 在工具栏上，选择**添加项 > 风险管理器 > 风险**。

   仅当您获得 IBM Security QRadar Risk Manager 的使用授权后，才会显示**风险管理器**仪表板项。
6. 在新的仪表板项标题上，单击黄色的**设置**图标。
7. 依次使用**图表类型**、**显示排名靠前的项**和**排序**列表来配置图表。
8. 从**组**列表中，选择要监视的组。 有关更多信息，请参阅步骤 9 中的表。

   选择**资产**选项后，指向**风险 > 策略管理 > 按资产**页面的链接显示在**风险**仪表板项的底部。 **按资产**页面显示为所选**策略组**返回的所有结果的更多详细信息。 有关特定资产的更多信息，请从**图表类型**列表中选择**表**并单击**资产**列中的链接以查看有关**按资产**页面中的资产的详细信息。

   选择**策略**选项后，指向**风险 > 策略管理 > 按策略**页面的链接显示在**风险**仪表板项的底部。 **按策略**页面显示为所选**策略组**返回的所有结果的更多详细信息。 有关特定策略的更多信息，请从**图表类型**列表中选择**表**并单击**策略**列中的链接以查看有关**按策略**页面中的策略的详细信息。
9. 从**图形**列表中，选择要使用的图形类型。 有关更多信息，请参阅下表:

组	传递的资产百分比	传递的策略检查百分比	传递的策略组百分比	策略风险分数
全部	返回资产、策略和策略组中的平均资产百分比传递速率。	返回资产、策略和策略组中的平均策略检查百分比传递速率。	返回所有资产、策略和策略组中的平均策略组传递速率。	返回所有资产、策略和策略组中的平均策略风险分数。
资产	返回资产是否传递资产合规性（100% = 已传递，0% = 失败）。 使用此设置可以显示哪些资产与策略组传递合规性相关联。	返回资产传递的策略检查的百分比。 使用此设置可以显示针对与策略组相关联的每个资产传递的策略检查的百分比。	返回与资产相关联的传递合规性的策略子组的百分比。	返回与每个资产相关联的策略问题的所有重要性因子值的总和。 使用此设置可以查看与所选策略组相关联的每个资产的策略风险。

组	传递的资产百分比	传递的策略检查百分比	传递的策略组百分比	策略风险分数
策略	返回是否所有与策略中的每项策略相关联的资产都传递合规性。 使用此设置可以监视是否所有与策略中的每项策略相关联的资产都进行传递。	返回按策略组中每项策略进行传递的策略检查的百分比。 使用此设置可以按每项策略监视失败的策略检查数。	返回策略所属的传递合规性的策略子组的百分比。	返回策略组中每个策略问题的重要性因子值。 使用此设置可以查看策略组中每项策略的重要性因子。
策略组	返回将所选组策略的合规性作为整体进行传递的资产的百分比。	返回按策略组的每项策略作为整体进行传递的策略检查的百分比。	返回策略组中传递合规性的策略子组的百分比。	返回策略组中所有策略问题的所有重要性因子值的总和。

10. 从**策略组**列表中，选择要监视的策略组。
11. 单击**保存**。

监视风险更改

创建用于显示所选资产、策略和策略组的每天、每周和每月的策略风险更改的仪表板项。

关于此任务

使用此仪表板项可以比较随时间推移策略组的策略风险分数、策略检查以及策略值中的更改。

风险更改仪表板项使用箭头来指示所选值的策略在所选时间段内增大、降低还是保持不变:

- 红色箭头下的数字表示显示风险增大的值。
- 灰色箭头下的数字表示风险未发生更改的值。
- 绿色箭头下的数字表示显示风险下降的值。

过程

1. 单击**仪表板**选项卡。
2. 在工具栏上，单击**新建仪表板**。
3. 输入历史策略合规性仪表板的名称和描述。
4. 单击**确定**。
5. 在工具栏上，选择**添加项 > 风险管理器 > 风险更改**。

   仅当您获得 IBM Security QRadar Risk Manager 的使用授权后，才会显示**风险管理器**仪表板项。
6. 在新的仪表板项标题上，单击黄色的**设置**图标。
7. 从**策略组**列表中，选择要监视的策略组。
8. 从**要比较的值**列表中选择选项:

- 如果要查看所选策略组中所有策略问题的重要性因子中的累积更改，请选择**策略风险分数**。
- 如果要查看所选策略组中哪些策略检查已更改，请选择**策略检查**。
- 如果要查看所选策略组中哪些策略已更改，请选择**策略**。

9. 从**变化量时间**列表中选择您要监视的风险更改时间段:
   - 如果要将今天凌晨 12:00 开始的风险更改与昨天的风险更改进行比较，请选择**天**。
   - 如果要将本周星期一凌晨 12:00 开始的风险更改与上周的风险更改进行比较，请选择**周**。
   - 如果要将本月第一天凌晨 12:00 开始的风险更改与上月的风险更改进行比较，请选择**月**。
10. 单击**保存**。

“漏洞管理”项

仅当您购买了 IBM Security QRadar Vulnerability Manager 并获得此产品的使用授权后，才会显示“漏洞管理”仪表板项。

有关更多信息，请参阅 *IBM Security QRadar Vulnerability Manager User Guide*。

可以根据**漏洞**选项卡中保存的搜索条件显示定制仪表板项。搜索项在**添加项 > 漏洞管理 > 漏洞搜索**菜单中列出。 搜索项的名称与该项所基于的已保存搜索条件的名称相匹配。

QRadar 提供了缺省的已保存搜索条件，此条件已预先配置为在**仪表板**选项卡菜单中显示搜索项。 您可以向**仪表板**选项卡菜单添加更多搜索仪表板项。

支持的图表类型包括表、饼图和条形图。 缺省图表类型为条形图。 这些图表可配置。

系统通知

“系统通知”仪表板项显示系统接收到的事件通知。

要使通知显示在**系统通知**仪表板项中，管理员必须创建一条基于每种通知消息类型的规则，并在“定制规则”向导中选中**通知**复选框。

有关如何配置事件通知以及创建事件规则的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

在“**系统通知**”仪表板项上，可以查看以下信息:

- **标志** - 显示一个符号，用于指示通知严重性级别。 将鼠标指针指向此符号可查看更多关于严重性级别的详细信息。
  - **运行状况**图标
  - **参考**图标 (?)
  - **错误**图标 (X)
  - **警告**图标 (!)
- **创建时间** - 显示自创建通知以来经过的时间长度。
- **描述** - 显示有关通知的信息。
- **“隐藏”图标 (x)** - 用于关闭系统通知。

通过将鼠标指针悬停在通知上，可以查看更多详细信息:

- **主机 IP** - 显示发出通知的主机的主机 IP 地址。
- **严重性** - 显示创建此通知的事故的严重性级别。
- **低级别类别** - 显示与生成此通知的事故相关联的低级别类别。 例如: 服务中断。
- **有效内容** - 显示与生成此通知的事故相关联的有效内容。
- **创建时间** - 显示自创建通知以来经过的时间长度。

添加**系统通知**仪表板项后，系统通知还可以在 QRadar 用户界面中显示为弹出通知。 这些弹出通知将显示在用户界面右下角，而与选择的选项卡无关。

弹出通知仅可供具有管理许可权的用户使用，并且缺省情况下处于启用状态。 要禁用弹出通知，请选择**用户首选项**，并取消选中**启用弹出通知**复选框。

在“系统通知”弹出窗口中，将突出显示队列中的通知数。 例如，如果标题中显示了 (1 - 12)，那么表明当前通知是即将显示的 12 个通知中的第一个通知。

“系统通知”弹出窗口提供了下列选项:

- **“下一个”图标 (>)** - 显示下一条通知消息。 例如，如果当前通知消息是 6 条消息中的第 3 条消息，那么单击此图标可以查看第 4 条消息。
- **“关闭”图标 (X)** - 关闭此通知弹出窗口。
- **（详细信息）** - 显示更多关于此系统通知的信息。

因特网威胁信息中心

“因特网威胁信息中心”仪表板项是一个嵌入式 RSS 订阅源，用于提供有关安全问题、每日威胁评估、安全新闻和威胁存储库的最新意见。

“当前威胁级别”图指示当前威胁级别，并提供了指向 IBM Internet Security Systems Web 站点的“当前因特网威胁级别”页面的链接。

此仪表板项中列出当前意见。要查看意见摘要，请单击意见旁边的**箭头**图标。这样该意见将展开以显示摘要。再次单击该**箭头**图标将隐藏摘要。

要查看完整的意见，请单击关联链接。IBM Internet Security Systems Web 站点将在另一浏览器窗口中打开，并显示完整的意见详细信息。

创建定制仪表板

您可以创建定制仪表板，以查看满足特定需求的仪表板项组。

关于此任务

创建定制仪表板后，新仪表板将显示在**仪表板**选项卡中，并在**显示仪表板**列表框中列出。 缺省情况下，新的定制仪表板为空仪表板；因此，您必须向其添加项。

过程

1. 单击**仪表板**选项卡。
2. 单击**新建仪表板**图标。
3. 在**名称**字段中，输入仪表板的唯一名称。 最大长度为 65 个字符。

4. 在**描述**字段中，输入仪表板的描述。 最大长度为 255 个字符。此描述将显示在**显示仪表板**列表框中仪表板名称的工具提示中。
5. 单击**确定**。

使用仪表板调查日志或网络活动

基于搜索的仪表板项提供了指向**日志活动**或**网络活动**选项卡的链接，从而使您能够进一步调查日志或网络活动。

关于此任务

要从**日志活动**仪表板项中调查流，请完成下列步骤:

1. 单击**在日志活动中查看**链接。 这将显示**日志活动**选项卡，其中显示了与仪表板项的参数匹配的结果和两个图表。

要从**网络活动**仪表板项中调查流，请完成下列步骤:

1. 单击**在网络活动中查看**链接。这将显示“网络活动”选项卡，其中显示了与仪表板项的参数匹配的结果和两个图表。

这将显示**网络活动**选项卡，其中显示了与仪表板项的参数匹配的结果和两个图表。 **日志活动**或**网络活动**选项卡上显示的图表类型取决于仪表板项中配置的图表:

图表类型	描述
条形图、饼图和表	**日志活动**或**网络活动**选项卡以条形图、饼图和表形式显示流详细信息。
时间序列	**日志活动**或**网络活动**选项卡根据以下条件显示图表: 1. 如果时间范围小于或等于 1 小时，那么将以时间序列图表、条形图以及表形式显示事件或流详细信息。 2. 如果时间范围大于 1 小时，那么将显示时间序列图表，并且将提示您单击“更新详细信息”。 此操作将启动用于填充事件或流详细信息的搜索，并生成条形图。 搜索完成后，将以条形图和表形式显示事件或流详细信息。

配置图表

如果适用，您可以配置**日志活动**、**网络活动**和**连接**仪表板项，以指定图表类型以及要查看的数据对象数。

关于此任务

表 11. 配置图表. 参数选项。

选项	描述
要绘图的值	在此列表框中，请选择要在图表上绘制的对象类型。 选项包括搜索参数中包含的所有规范化以及定制事件或流参数。

表 11. 配置图表 (续). 参数选项。

选项	描述
图表类型	在此列表框中，请选择要查看的图表类型。 选项包括: 1. **条形图** - 以条形图形式显示数据。此选项仅可用于已分组事件或流。 2. **饼图** - 以饼图形式显示数据。此选项仅可用于已分组事件或流。 3. **表** - 以表格形式显示数据。 此选项仅可用于已分组事件或流。 4. **时间序列** - 显示交互式折线图，此图代表指定的时间间隔所匹配的记录。
显示排名靠前的项	在此列表框中，请选择要在图表中查看的对象数。 选项包括 **5** 和 **10**。 缺省值为 **10**。
捕获时间序列数据	选中此复选框可启用时间序列捕获。 选中此复选框后，图表功能将开始累积时间序列图表的数据。 缺省情况下，此选项处于禁用状态。
时间范围	在此列表框中，请选择要查看的时间范围。

您的定制图表配置已保留，因此每次访问**仪表板**选项卡时，这些配置将显示为已配置。

数据可以进行累积，以便当您执行保存的时间序列搜索时，事件或流数据的高速缓存可用于显示上一时间段的数据。累积的参数在**要绘图的值**列表框中以星号 (*) 指示。 如果选择的要绘图的值不进行累积（没有星号），那么时间序列数据不可用。

过程

1. 单击**仪表板**选项卡。
2. 从**显示仪表板**列表框中，选择包含要定制的项的仪表板。
3. 在要配置的仪表板项的标题中，单击**设置**图标。
4. 配置图表参数。

除去仪表板项

您可以从仪表板中除去项，以及随时重新添加项。

关于此任务

从仪表板中除去某项时，该项不会完全除去。

过程

1. 单击**仪表板**选项卡。
2. 从**显示仪表板**列表框中，选择要从中除去项的仪表板。
3. 在仪表板项标题上，单击红色的 [x] 图标以将该项从仪表板中除去。

拆离仪表板项

您可以拆离仪表板中的项，并将该项显示在桌面系统上的新窗口中。

关于此任务

拆离仪表板项后，原始仪表板项仍显示在**仪表板**选项卡上，而包含仪表板项副本的拆离窗口将保持打开，并按照安排的时间间隔进行刷新。 即使您将 QRadar 应用程序关闭，拆离的窗口也将保持打开状态以进行监视，并继续进行刷新，直到您手动关闭此窗口或关闭计算机系统为止。

过程

1. 单击**仪表板**选项卡。
2. 从**显示仪表板**列表框中，选择要从中拆离项的仪表板。
3. 在仪表板项标题上，单击绿色图标以拆离该仪表板项，然后在另一窗口中将其打开。

重命名仪表板

您可以重命名仪表板并更新描述。

过程

1. 单击**仪表板**选项卡。
2. 从**显示仪表板**列表框中，选择要编辑的仪表板。
3. 在工具栏中，单击**重命名仪表板**图标。
4. 在**名称**字段中，输入仪表板的新名称。 最大长度为 65 个字符。
5. 在**描述**字段中，输入仪表板的新描述。 最大长度为 255 个字符。
6. 单击**确定**。

删除仪表板

您可以删除仪表板。

关于此任务

删除仪表板后，**仪表板**选项卡将进行刷新，并且将显示**显示仪表板**列表框中列出的第一个仪表板。 已删除的仪表板将不再显示在**显示仪表板**列表框中。

过程

1. 单击**仪表板**选项卡。
2. 从**显示仪表板**列表框中，选择要删除的仪表板。
3. 在工具栏中，单击**删除仪表板**。
4. 单击**是**。

管理系统通知

您可以指定要在**系统通知**仪表板项上显示的通知数，并在阅读这些通知后将其关闭。

开始之前

确保已将**系统通知**仪表板项添加到仪表板中。

过程

1. 在“系统通知”仪表板项标题上，单击**设置**图标。
2. 从**显示**列表框中，选择要查看的系统通知数。
   - 选项包括 **5**、**10**（缺省值）、**20**、**50** 和**全部**。
   - 要查看过去 24 小时内记录的所有系统通知，请单击**全部**。
3. 要关闭系统通知，请单击**删除**图标。

向“添加项”列表添加基于搜索的仪表板项

您可以向**添加项**菜单添加基于搜索的仪表板项。

开始之前

要向**仪表板**选项卡上的**添加项**菜单添加事件和流搜索仪表板项，必须访问**日志活动**或**网络活动**选项卡，以创建指定搜索结果可以在**仪表板**选项卡中显示的搜索条件。另外，搜索条件还必须指定结果按某个参数进行分组。

过程

1. 选择:
   - 要添加流搜索仪表板项，请单击**网络活动**选项卡。
   - 要添加事件搜索仪表板项，请单击**日志活动**选项卡。
2. 从**搜索**列表框中，选择下列其中一个选项:
   - 要创建搜索，请选择**新建搜索**。
   - 要编辑已保存的搜索，请选择**编辑搜索**。
3. 根据需要配置或编辑搜索参数。
   - 在“编辑搜索”窗格上，选中**包括在仪表板中**选项。
   - 在“列定义”窗格上，选择某一列，然后单击**添加列**图标，以将该列移动到**分组依据**列表。
4. 单击**过滤**。 这将显示搜索结果。
5. 单击**保存条件**。 请参阅“在攻击选项卡上保存搜索条件”。
6. 单击**确定**。
7. 验证已保存的搜索条件是否已成功地将事件或流搜索仪表板项添加到**添加项**列表。
   a. 单击**仪表板**选项卡。
   b. 选择下列其中一个选项:
   a. 要验证事件搜索项，请选择**添加项** > **日志活动** > **事件搜索** > **添加项**。
   b. 要验证流搜索项，请选择**添加项** > **网络活动** > **流搜索**。 仪表板项将显示在与已保存的搜索条件同名的列表中。

第 4 章 攻击管理

同一个攻击中目标 IP 地址跨多个网络的事件和流可能相互关联。您可以有效地调查网络中的各个攻击。

限制: 您不能管理 IBM Security QRadar Log Manager 中的攻击。有关 IBM Security QRadar SIEM 与 IBM Security QRadar Log Manager 之间的差异的更多信息，请参阅第 5 页的『安全情报产品中的功能』。

您可以浏览**攻击**选项卡的各个页面以调查事件和流详细信息，从而确定引起攻击的唯一事件和流。

攻击概述

通过使用**攻击**选项卡，可以调查网络中的攻击、源和目标 IP 地址、网络行为及异常。

您还可以根据各项条件搜索攻击。 有关搜索攻击的更多信息，请参阅第 140 页的『攻击搜索』。

攻击许可权注意事项

无论攻击与哪个日志源或流源关联，所有用户都可以查看所有攻击。

攻击选项卡不使用设备级别用户许可权来确定各个用户能够查看的攻击；这由网络许可权确定。

有关设备级别许可权的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

关键术语

通过使用**攻击**选项卡，您可以访问以及分析攻击、源 IP 地址和目标 IP 地址。

项	描述
攻击	一个攻击包含多个来自于一个源（例如主机或日志源）的事件或流。**攻击**选项卡用于显示攻击，其中包括流量以及进行协作并对攻击规模进行验证的漏洞。攻击规模由每次重新评估攻击时对其执行的多项测试确定。重新评估在事件添加到攻击时按调度的时间间隔进行。
源 IP 地址	源 IP 地址指定网络中尝试破坏组件安全性的设备。源 IP 地址可以使用各种攻击方法（例如侦察或拒绝服务 (DoS) 攻击）来尝试进行未经授权的访问。
目标 IP 地址	目标 IP 地址指定源 IP 地址所尝试访问的网络设备。

攻击保留时间

在**管理**选项卡上，可以配置攻击保留期系统设置，以便在配置的时间段后从数据库中除去攻击。

缺省攻击保留期为 3 天。您必须具有管理许可权才能访问“**管理**”选项卡和配置系统设置。配置阈值时，定义的任何阈值将增加 5 天。

关闭攻击后，已关闭的攻击将在攻击保留期过后从数据库中除去。如果针对某个攻击又发生了一些事件，那么将创建新攻击。如果执行的搜索包括已关闭的攻击，那么搜索结果中会显示未从数据库中除去的项。

攻击监视

通过使用**攻击**选项卡中提供的不同视图，可以监视攻击以确定网络中当前发生的攻击。

将列出攻击，规模最大的攻击排列在最前面。您可以查找并查看特定攻击的详细信息，然后根据需要对该攻击执行操作。

开始浏览各个视图后，选项卡顶部将显示当前视图的导航轨迹。如果要返回到先前查看的页面，请在导航轨迹上单击页面名称。

从**攻击**选项卡上的导航菜单中，可以访问下表中列出的下列页面。

*表 12. 可从**攻击**选项卡访问的页面*

页面	描述
我的攻击	显示分配给您的所有攻击。
所有攻击	显示网络中的所有全局攻击。
按类别	显示按高级别和低级别类别分组的所有攻击。
按源 IP	显示按攻击中涉及的源 IP 地址分组的所有攻击。
按目标 IP	显示按攻击中涉及的目标 IP 地址分组的所有攻击。
按网络	显示按攻击中涉及的网络分组的所有攻击。
规则	提供对“规则”页面的访问，您可以在此页面中查看和创建定制规则。仅当您具有“查看定制规则”角色许可权时，才会显示此选项。有关更多信息，请参阅规则管理。

监视“所有攻击”或“我的攻击”页面

您可以在“所有攻击”或“我的攻击”页面上监视攻击。

开始之前

“所有攻击”页面显示网络中正在发生的所有攻击的列表。 “我的攻击”页面显示指定给您的攻击的列表。

关于此任务

表顶部显示应用于搜索结果的攻击搜索参数（如果有）的详细信息。 要清除这些搜索参数，您可以单击**清除过滤器**。有关搜索攻击的更多信息，请参阅攻击搜索。

注: 要更详细地查看“摘要”页面上的窗格，请单击相关联的工具栏选项。 例如，如果要查看源 IP 地址的详细信息，请单击**源**。 有关工具栏选项的更多信息，请参阅“攻击”选项卡工具栏功能。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，选择**所有攻击**或**我的攻击**。
3. 您可以使用以下选项优化攻击列表:
   - 从**查看攻击**列表框中，选择相应的选项，用于过滤攻击列表以获取特定时间范围的攻击。
   - 单击**当前搜索参数**窗格中显示的每个过滤器旁的**清除过滤器**链接。
4. 双击要查看的攻击。
5. 在“攻击摘要”页面上，查看攻击详细信息。 请参阅攻击参数。
6. 对该攻击执行任何必要操作。

监视按类别分组的攻击

您可以在“按类别”详细信息页面上监视攻击，此页面提供了按高级别类别分组的攻击列表。

关于此任务

计数字段（例如，**事件计数**、**流计数**和**源计数**）不考虑用户的网络许可权。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**按类别**。
3. 要查看特定高级别类别的低级别类别组，请单击高级别类别名称旁边的箭头图标。
4. 要查看低级别类别的攻击列表，请双击低级别类别。
5. 双击要查看的攻击。
6. 在“攻击摘要”页面上，查看攻击详细信息。 请参阅攻击参数。
7. 对该攻击执行任何必要操作。 请参阅攻击管理任务。

监视按源 IP 分组的攻击

在“源”页面上，可以监视按源 IP 地址分组的攻击。

关于此任务

源 IP 地址指定由于系统遭受攻击而生成攻击的主机。 所有源 IP 地址都将列出，攻击规模最大的源 IP 地址排列在最前面。攻击列表仅显示具有活动攻击的源 IP 地址。

过程

1. 单击**攻击**选项卡。
2. 单击**按源 IP**。
3. 您可以使用以下选项优化攻击列表:
   - 从**查看攻击**列表框中，选择相应的选项，用于过滤攻击列表以获取特定时间范围的攻击。
   - 单击**当前搜索参数**窗格中显示的每个过滤器旁的**清除过滤器**链接。
4. 双击要查看的组。
5. 要查看源 IP 地址的本地目标 IP 地址列表，请在“源”页面工具栏上单击**目标**。
6. 要查看与此源 IP 地址相关联的攻击列表，请在“源”页面工具栏上单击**攻击**。
7. 双击要查看的攻击。
8. 在“攻击摘要”页面上，查看攻击详细信息。 请参阅攻击参数。
9. 对该攻击执行任何必要操作。 请参阅攻击管理任务。

监视按目标 IP 分组的攻击

在“目标”页面上，可以监视按本地目标 IP 地址分组的攻击。

关于此任务

所有目标 IP 地址都将列出，攻击规模最大的目标 IP 地址排列在最前面。

过程

1. 单击**攻击**选项卡。
2. 单击**按目标 IP**。
3. 您可以使用以下选项优化攻击列表:
   - 从**查看攻击**列表框中，选择相应的选项，用于过滤攻击列表以获取特定时间范围的攻击。
   - 单击**当前搜索参数**窗格中显示的每个过滤器旁的**清除过滤器**链接。
4. 双击要查看的目标 IP 地址。
5. 要查看与此目标 IP 地址相关联的攻击列表，请在“目标”页面工具栏上单击**攻击**。
6. 要查看与此目标 IP 地址相关联的源 IP 地址列表，请在“目标”页面工具栏上单击**源**。
7. 双击要查看的攻击。
8. 在“攻击摘要”页面上，查看攻击详细信息。 请参阅攻击参数。
9. 对该攻击执行任何必要操作。 请参阅攻击管理任务。

监视按网络分组的攻击

在“网络”页面上，可以监视按网络分组的攻击。

关于此任务

所有网络都将列出，攻击规模最大的网络排列在最前面。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**按网络**。
3. 双击要查看的网络。
4. 要查看与此网络相关联的源 IP 地址列表，请在“网络”页面工具栏上单击**源**。
5. 要查看与此网络相关联的目标 IP 地址列表，请在“网络”页面工具栏上单击**目标**。
6. 要查看与此网络相关联的攻击列表，请在“网络”页面工具栏上单击**攻击**。
7. 双击要查看的攻击。
8. 在“攻击摘要”页面上，查看攻击详细信息。 请参阅攻击参数。
9. 对该攻击执行任何必要操作。 请参阅攻击管理任务。

攻击管理任务

监视攻击时，可以对攻击执行操作。

您可以执行下列操作:

- 添加备注
- 除去攻击
- 保护攻击
- 将攻击数据导出为 XML 或 CSV
- 将攻击分配给其他用户
- 发送电子邮件通知
- 将攻击标记为需要跟进
- 隐藏或关闭任何攻击列表中的攻击

要对多个攻击执行某个操作，请按住 Control 键并选择要选中的各个攻击。要在新页面上查看攻击详细信息，请按住 Control 键并双击攻击。

添加备注

您可以向**攻击**选项卡上的任何攻击添加备注。 备注可以包含要为攻击捕获的信息，例如，客户支持凭单号或攻击管理信息。

关于此任务

备注最多可以包含 2000 个字符。

过程

1. 单击**攻击**选项卡。
2. 浏览到要向其添加备注的攻击。
3. 双击该攻击。
4. 从**操作**列表框中，选择**添加备注**。
5. 输入要针对此攻击包含的备注。
6. 单击**添加备注**。

结果

备注将显示在“攻击摘要”上的“最后 5 条备注”窗格中。 **攻击**列表的“标志”列中将显示**备注**图标。如果将鼠标悬停在**攻击**列表的**标志**列中的备注指示符上，那么将显示该攻击的备注。

隐藏攻击

要避免攻击显示在**攻击**选项卡中，您可以将其隐藏。

关于此任务

隐藏攻击后，此攻击将不再显示在**攻击**选项卡上的任何列表（例如“所有攻击”）中；但是，如果执行包含隐藏攻击的搜索，那么搜索结果将显示该项。

过程

1. 单击**攻击**选项卡。
2. 单击**所有攻击**。
3. 选择要隐藏的攻击。
4. 从**操作**列表框中，选择**隐藏**。
5. 单击**确定**。

显示处于隐藏状态的攻击

处于隐藏状态的攻击在**攻击**选项卡上不可见，但是，如果要重新查看处于隐藏状态的攻击，那么可以显示这些攻击。

关于此任务

要显示处于隐藏状态的攻击，您必须执行包含处于隐藏状态的攻击的搜索。 搜索结果包括所有攻击，其中包括处于隐藏状态和未处于隐藏状态的攻击。 攻击通过**标志**列中的**已隐藏**图标指定为处于隐藏状态。

过程

1. 单击**攻击**选项卡。
2. 单击**所有攻击**。
3. 搜索处于隐藏状态的攻击:
   a. 从**搜索**列表框中，选择**新建搜索**。
   b. 在“搜索参数”窗格上的**排除选项**列表中，取消选中**处于隐藏状态的攻击**复选框。
   c. 单击**搜索**。
4. 查找并选择要显示的处于隐藏状态的攻击。
5. 从**操作**列表框中，选择**显示**。

关闭攻击

要将攻击从系统中完全除去，您可以关闭此攻击。

关于此任务

关闭（删除）攻击后，这些攻击将不会在**攻击**选项卡上的任何列表（例如，“所有攻击”）中显示。已关闭的攻击将在攻击保留期过后从数据库中除去。 缺省攻击保留期为 3 天。 如果针对某个攻击发生了多个事件，那么将创建新攻击。 如果执行的搜索包括已关闭的攻击，那么搜索结果将显示未从数据库中除去的项。

关闭攻击时，必须选择关闭攻击的原因，并且可以添加备注。 **备注**字段显示针对上一攻击关闭输入的备注。 备注长度不得超过 2,000 个字符。此备注将显示在此攻击的“备注”窗格中。 如果您具有“管理攻击关闭”许可权，那么可以向**关闭原因**列表框添加新的定制原因。

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

过程

1. 单击**攻击**选项卡。
2. 单击**所有攻击**。
3. 选择下列其中一个选项:
   - 选择要关闭的攻击，然后从**操作**列表框中选择**关闭**。
   - 从**操作**列表框中，选择**关闭列示项**。
4. 从**关闭原因**列表框中，选择原因。 缺省原因是**不重要的问题**。
5. 可选。 在**备注**字段中输入备注，以提供更多关于关闭备注的信息。
6. 单击**确定**。

结果

关闭攻击后，**攻击**选项卡的“按类别排列”窗格上显示的计数需要花费几分钟的时间才能反映已关闭的攻击。

保护攻击

可以避免在保留期过后将攻击从数据库中除去。

关于此任务

攻击将保留一段时间，这段时间称为保留期，并且可配置。缺省保留期为 3 天；但是，管理员可以对保留期进行定制。 可能存在需要保留而与保留期无关的攻击。 可以避免在保留期过后将这些攻击从数据库中除去。

有关攻击保留期的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

注意:
通过“硬清除”选项重置 SIM 数据模型后，将从数据库和磁盘中除去所有攻击（包括受保护的攻击）。 您必须具有管理特权才能重置 SIM 数据模型。

过程

1. 单击**攻击**选项卡。
2. 单击**所有攻击**。
3. 选择下列其中一个选项:

- 选择要保护的攻击，然后从**操作**列表框中选择**保护**。
- 从**操作**列表框中，选择**保护列示项**。

4. 单击**确定**。

结果

受保护的攻击由**标志**列中的**受保护**图标指示。

取消保护攻击

在攻击保留期经过之后，您可以取消保护先前免遭除去的攻击。

关于此任务

要仅列出受保护的攻击，您可以执行过滤结果仅包含受保护攻击的搜索。 如果取消选中**受保护**复选框，并确保在“搜索参数”窗格上的**排除选项**列表下选择了所有其他选项，那么将仅显示受保护的攻击。

过程

1. 单击**攻击**选项卡。
2. 单击**所有攻击**。
3. 可选。 执行仅显示受保护攻击的搜索。
4. 选择下列其中一个选项:
   - 选择要保护的攻击，然后从“操作”列表框中选择**取消保护**。
   - 从**操作**列表框中，选择**取消保护列示项**。
5. 单击**确定**。

导出攻击

您可以采用可扩展标记语言 (XML) 格式或逗号分隔值 (CSV) 格式导出攻击。

关于此任务

如果要复用或存储攻击数据，您可以导出攻击。 例如，可以导出攻击以创建并非基于 QRadar 产品的报告。 另外，还可以作为辅助的长期保留策略而导出攻击。 客户支持人员可能会要求您导出攻击以进行故障诊断。

生成的 XML 或 CSV 文件包含搜索参数的“列定义”窗格中指定的参数。 导出数据所需的时间长度取决于指定的参数数目。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**所有攻击**。
3. 选择要导出的攻击。
4. 选择下列其中一个选项:
   - 要以 XML 格式导出攻击，请从“操作”列表框中选择**操作 > 导出为 XML**。
   - 要以 CSV 格式导出攻击，请从“操作”列表框中选择**操作 > 导出为 CSV**。
5. 选择下列其中一个选项:

- 要打开列表以便立即查看，请选择**打开方式**选项，然后从列表框中选择应用程序。
- 要保存列表，请选择**保存到磁盘**选项。

6. 单击**确定**。

将攻击分配给用户

通过使用**攻击**选项卡，可以将攻击分配给用户以进行调查。

关于此任务

向用户分配攻击时，攻击将显示在属于该用户的“我的攻击”页面上。 您必须具有相应的特权才能将攻击分配给用户。

您可以通过**攻击**选项卡或“攻击摘要”页面将攻击分配给用户。此过程提供有关如何通过**攻击**选项卡分配攻击的指示信息。

注: **用户名**列表框将仅显示那些具有**攻击**选项卡特权的用户。

过程

1. 单击**攻击**选项卡。
2. 单击**所有攻击**。
3. 选择要分配的攻击。
4. 从**操作**列表框中，选择**分配**。
5. 从**用户名**列表框中，选择要将此攻击分配到的用户。
6. 单击**保存**。

结果

此攻击将分配给所选用户。 **用户**图标将显示在**攻击**选项卡的“标志”列中，以指示已分配此攻击。指定用户可以在其“我的攻击”页面中查看其攻击。

发送电子邮件通知

您可以向任何有效电子邮件地址发送包含攻击摘要的电子邮件。

关于此任务

电子邮件的正文包含以下信息（如果有）：

- 源 IP 地址
- 源用户名、主机名或资产名称
- 源的总数
- 排名前 5 位的源（按规模排列）
- 源网络
- 目标 IP 地址
- 目标用户名、主机名或资产名称
- 目标总数
- 排名前 5 位的目标（按规模排列）

- 目标网络
- 事件总数
- 导致攻击或事件规则触发的规则
- 攻击或事件规则的完整描述
- 攻击标识
- 排名前 5 位的类别
- 攻击的开始时间或生成事件的时间
- 排名前 5 位的注释
- 指向攻击用户界面的链接
- 添加内容的 CRE 规则

过程

1. 单击**攻击**选项卡。
2. 浏览到要针对其发送电子邮件通知的攻击。
3. 双击该攻击。
4. 从**操作**列表框中，选择**电子邮件**。
5. 配置以下参数:

选项	描述
参数	描述
收件人	请输入所选攻击发生更改时要通知的用户的电子邮件地址。 请使用逗号分隔多个电子邮件地址。
发件人	请输入缺省的发端电子邮件地址。 缺省值为 root@localhost.com。
电子邮件主题	请输入电子邮件的缺省主题。 缺省值为攻击标识。
电子邮件消息	请输入要随通知电子邮件一起发送的标准消息。

6. 单击**发送**。

将项标记为需要跟进

通过使用**攻击**选项卡，可以将攻击、源 IP 地址、目标 IP 地址和网络标记为需要跟进。这使您能够跟踪特定项以展开进一步调查。

过程

1. 单击**攻击**选项卡。
2. 浏览到要标记为需要跟进的攻击。
3. 双击该攻击。
4. 从**操作**列表框中，选择**跟进**。

结果

现在，该攻击在**标志**列中显示了一个标志，这表示已将该攻击标记为需要跟进。 如果您在攻击列表中看不到标记的攻击，可以对此列表进行排序，以首先显示所有已标记的攻击。 要按已标记的攻击对攻击列表进行排序，请双击**标志**列标题。

“攻击”选项卡工具栏的功能

攻击选项卡上的每个页面和表都有一个工具栏，用于提供执行特定操作或调查攻击的构成要素所需的功能。

表 13. “攻击”选项卡工具栏的功能

功能	描述
添加备注	单击**添加备注**可以向攻击添加新备注。此选项仅在“攻击摘要”页面的“最后 5 条备注”窗格上可用
操作	**操作**列表框中的可用选项随页面、表或项（例如攻击或源 IP 地址）不同而有所变化。**操作**列表框的显示内容可能与下面列出的内容并不完全相同。 从**操作**列表框中，您可以选择下列其中一项操作: • **跟进** - 选择此选项可以标记要进一步跟进的项。请参阅标记项以便跟进。 • **隐藏** - 选择此选项可以隐藏攻击。有关隐藏攻击的更多信息，请参阅隐藏攻击。 • **显示** - 选择此选项可以显示所有隐藏的攻击。 • **保护攻击** - 选择此选项可以保护攻击。有关保护攻击的更多信息，请参阅保护攻击。 • **关闭** - 选择此选项可以关闭攻击。有关关闭攻击的更多信息，请参阅关闭攻击。 • **关闭列示项** - 选择此选项可以关闭列示的攻击。有关关闭列示的攻击的更多信息，请参阅关闭攻击。 • **电子邮件** - 选择此选项可以通过电子邮件将攻击摘要发送给一位或多位收件人。请参阅发送电子邮件通知。 • **添加备注** - 选择此选项可以为项添加备注。请参阅添加备注。 • **分配** - 选择此选项可以向用户分配攻击。请参阅向用户分配攻击。 • **打印** - 选择此选项可以打印攻击信息

表 13. “攻击”选项卡工具栏的功能 (续)

功能	描述
注释	单击**注释**可以查看攻击的所有注释。 • **注释** - 指定注释详细信息。注释是规则可以对攻击自动添加的文本描述，作为规则响应的组成部分。 • **时间** - 指定创建注释的日期及时间。
异常	单击**异常**可以显示导致异常检测规则生成攻击的已保存搜索结果。 **注**: 仅当攻击由异常检测规则生成时，才会显示此按钮。
类别	单击**类别**可以查看攻击的类别信息。 要进一步调查与特定类别有关的事件，您还可以右键单击类别，然后选择**事件**或**流**。另外，也可以突出显示类别，然后在“事件类别列表”工具栏中单击**事件**或**流**图标。
连接	单击**连接**可以对连接进行进一步调查。 **注**: 仅当您购买了 IBM Security QRadar Risk Manager 并获得此产品的使用授权后，此选项才可用。有关更多信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。 单击**连接**图标时，将在新页面上显示连接搜索条件页面，其中预先填写了事件搜索条件。 需要时，您可以对搜索参数进行定制。单击**搜索**可以查看连接信息。
目标	单击**目标**可以查看攻击、源 IP 地址或网络的所有本地目标 IP 地址。 **注**: 如果目标 IP 地址位于远程位置，那么将打开一个单独的页面，其中提供了远程目标 IP 地址的信息。
显示	“攻击摘要”页面显示多个与攻击有关的信息表。要定位到某个表，可以滚动到要查看的表，也可以从**显示**列表框中选择对应选项。
事件	单击**事件**可以查看攻击的所有事件。您单击**事件**时，将显示事件搜索结果。
流	单击**流**可以对攻击的关联流进行进一步调查。您单击**流**时，将显示流搜索结果。
日志源	单击**日志源**可以查看攻击的所有日志源。
网络	单击**网络**可以查看攻击的所有目标网络。
备注	单击**备注**可以查看攻击、源 IP 地址、目标 IP 地址或网络的所有备注。有关备注的更多信息，请参阅添加备注
攻击	单击**攻击**可以查看与源 IP 地址、目标 IP 地址或网络关联的攻击列表。
打印	单击**打印**可以打印攻击信息。

表 13. “攻击”选项卡工具栏的功能 (续)

功能	描述
规则	单击**规则**可以查看所有添加到攻击的规则。创建攻击的规则最先列出。 如果您具有编辑规则所需的相应许可权，那么双击该规则将启动“编辑规则”页面。 对于已删除的规则，该规则旁边将显示一个红色图标 (x)。如果双击已删除的规则，那么将显示一条消息，指出该规则不再存在。
保存条件	执行攻击搜索后，单击**保存条件**可以保存搜索条件以供将来使用。
保存布局	缺省情况下，“按类别”详细信息页面按“攻击计数”参数进行排序。如果您更改了排序顺序或者按其他参数进行排序，请单击**保存布局**，以便将当前显示保存为缺省视图。您下次登录**攻击**选项卡时，将显示已保存的布局。
搜索	此选项仅在“本地目标列表”表工具栏中可用。 单击**搜索**可以对源 IP 地址的目标 IP 进行过滤。要过滤目标，请完成下列步骤: 1. 单击**搜索**。 2. 输入下列参数的值: • **目标网络** - 在此列表框中，请选择要过滤的网络。 • **规模** - 在此列表框中，请选择是要根据等于、小于还是大于所配置值的规模进行过滤。 • **排序依据** - 在此列表框中，请选择如何对过滤结果进行排序。 3. 单击**搜索**。
显示不活动类别	在“按类别”详细信息页面上，每个类别的计数都从低级别类别中的值开始进行累计。具有关联攻击的低级别类别显示为带有箭头。您可以单击此箭头以查看关联的低级别类别。如果要查看所有类别，请单击**显示不活动类别**。
源	单击**源**可以查看攻击、目标 IP 地址或网络的所有源 IP 地址。
摘要	如果您已单击了**显示**列表框中的某个选项，那么可以单击**摘要**以返回到详细摘要视图。
用户	单击**用户**可以查看与某个攻击关联的所有用户。

表 13. “攻击”选项卡工具栏的功能 (续)

功能	描述
查看攻击路径	单击**查看攻击路径**可以对攻击的攻击路径进行进一步调查。您单击**查看攻击路径**图标时，将在新页面中显示“当前拓扑”页面。 **注**: 仅当您购买了 IBM Security QRadar Risk Manager 并获得此产品的使用授权后，此选项才可用。有关更多信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。
查看拓扑	单击**查看拓扑**可以对攻击源进行进一步调查。单击**查看拓扑**图标时，将在新页面中显示“当前拓扑”页面。 **注**: 仅当您购买了 IBM Security QRadar Risk Manager 并获得此产品的使用授权后，此选项才可用。有关更多信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。

攻击参数

下表提供“攻击”选项卡中提供的参数的描述。

表 14. 攻击参数

参数	位置	描述
注释	“排名前 5 位的注释”表	指定注释详细信息。注释是规则可以对攻击自动添加的文本描述，作为规则响应的组成部分。
异常	“最后 10 个事件（异常事件）”表	选中此选项可以显示导致异常检测规则生成事件的已保存搜索结果。
异常文本	“最后 10 个事件（异常事件）”表	指定对异常检测规则所检测到的异常行为的描述。
异常值	“最后 10 个事件（异常事件）”表	指定导致异常检测规则生成攻击的值。
应用程序	“最后 10 个流”表	指定与流关联的应用程序。
应用程序名称	“攻击源”表（如果攻击类型是“应用程序标识”）	指定与创建攻击的流关联的应用程序。
ASN 索引	“攻击源”表（如果攻击类型是“源 ASN”或“目标 ASN”）	指定与创建攻击的流关联的 ASN 值。
资产名称	“攻击源”表（如果攻击类型是“源 IP”或“目标 IP”）	指定可使用“资产概要文件”功能分配的资产名称。有关更多信息，请参阅资产管理。
资产权重	“攻击源”表（如果攻击类型是“源 IP”或“目标 IP”）	指定可使用“资产概要文件”功能分配的资产权重。有关更多信息，请参阅资产管理。

表 14. 攻击参数 (续)

参数	位置	描述
分配给	“攻击”表	指定分配给攻击的用户。 如果未分配用户，那么此字段指定“未分配”。单击“未分配”可向用户分配攻击。有关更多信息，请参阅将攻击分配给用户。
类别	“最后 10 个事件”表	指定事件的类别。
类别名称	“按类别排列”详细信息页面	指定高级别类别名称。
已链接	• “攻击源”表（如果攻击类型是“目标 IP”） • “排名前 5 位的目标 IP”表	指定是否链接了目标 IP 地址。 链接的目标 IP 地址与其他攻击关联。例如，目标 IP 地址可以变为另一攻击的源 IP 地址。如果链接了目标 IP 地址，请单击**是**以查看链接的攻击。
创建日期	“最后 5 条备注”表	指定创建备注的日期和时间。
可信性	“攻击”表	指定攻击的可信性，其值由源设备中的可信性评级确定。例如，当多个攻击报告同一事件或流时，可信性将增加。
当前搜索参数	• “按源 IP 排列”详细信息页面 • “按目标 IP 排列”详细信息页面	表顶部显示应用于搜索结果的搜索参数的详细信息。要清除这些搜索参数，请单击**清除过滤器**。 **注**：仅当您应用过滤器后，才会显示此参数。
描述	• “所有攻击”页面 • “我的攻击”页面 • “攻击”表 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面 • “攻击源”表（如果攻击类型是“日志源”） • “排名前 5 位的日志源”表	指定攻击或日志源的描述。
目标 IP	• “最后 10 个事件”表 • “最后 10 个流”表	指定事件或流的目标 IP 地址。

表 14. 攻击参数 (续)

参数	位置	描述
目标 IP	• “排名前 5 位的目标 IP”表 • “按源 IP 排列 - 本地目标列表”页面 • “按目标 IP 排列”详细信息页面 • “按网络排列 - 本地目标列表”页面	指定目标的 IP 地址。如果在“管理”选项卡上启用了 DNS 查找，那么可以通过将鼠标悬停在 IP 地址上方来查看 DNS 名称。
目标 IP	“攻击”表	指定本地或远程目标的 IP 地址和资产名称（如果可用）。单击此链接可查看更多详细信息。
目标 IP	• “所有攻击”页面 • “我的攻击”页面	指定本地或远程目标的 IP 地址和资产名称（如果可用）。如果多个目标 IP 地址与攻击关联，那么此字段指定“多个”以及目标 IP 地址数。
目标 IP	• “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面	指定与攻击关联的目标的 IP 地址和资产名称（如果可用）。如果在“管理”选项卡上启用了 DNS 查找，那么可以通过将鼠标悬停在 IP 地址或资产名称上方来查看 DNS 名称。
目标 IP	“按网络排列”详细信息页面	指定与网络关联的目标 IP 地址数。
目标端口	“最后 10 个流”表	指定流的目标端口。
目标	• “排名前 5 位的源 IP”表 • “按源 IP 排列”详细信息页面 • “按目标 IP 排列 - 源列表”页面 • “按网络排列 - 源列表”页面	指定 QID 图中标识的事件名称，该名称与创建攻击的事件或流关联。将鼠标悬停在事件名称上方可查看 QID。
事件/流计数	“按类别排列”详细信息页面	指定与类别中的攻击关联的活动事件或流（未关闭或未处于隐藏状态的事件或流）数量。 如果未接收到新事件或流，那么攻击将仅在一段时间内保持活动状态。攻击将仍然显示在“攻击”选项卡中，但不会计入此字段。

表 14. 攻击参数 (续)

参数	位置	描述
事件/流计数	“目标”页面 “网络”页面	指定针对攻击发生的事件和流数量以及类别数。 单击事件链接可对与攻击关联的事件展开进一步调查。单击事件链接时，将显示事件搜索结果。 单击流链接可对与攻击关联的流展开进一步调查。单击流链接时，将显示流搜索结果。 **注**：如果流计数显示“不适用”，那么攻击的开始日期可能早于将 QRadar 产品升级到 V7.1.0 (MR1) 的日期。因此，无法对流进行计数。但是，您可以单击“不适用”链接以调查流搜索结果中的关联流。
事件/流计数	“按类别排列”详细信息页面	指定与类别中的攻击关联的活动事件或流（未关闭或未处于隐藏状态的事件或流）数量。 如果未接收到新事件或流，那么攻击将仅在一段时间内保持活动状态。攻击将仍然显示在“攻击”选项卡中，但不会计入此字段。
事件/流计数	“目标”页面 “网络”页面	指定针对攻击发生的事件和流数量以及类别数。 单击事件链接可对与攻击关联的事件展开进一步调查。单击事件链接时，将显示事件搜索结果。 单击流链接可对与攻击关联的流展开进一步调查。单击流链接时，将显示流搜索结果。 **注**：如果流计数显示“不适用”，那么攻击的开始日期可能早于将 QRadar 产品升级到 V7.1.0 (MR1) 的日期。因此，无法对流进行计数。但是，您可以单击“不适用”链接以调查流搜索结果中的关联流。

表 14. 攻击参数 (续)

参数	位置	描述
事件数量	• “所有攻击”页面 • “我的攻击”页面 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面	指定攻击的事件数。
事件/流数量	• “攻击源”表（如果攻击类型是“源 IP”、“目标 IP”、“主机名”、“用户名”、“源端口”或“目标端口”、“事件名称”、“端口”、“源 MAC 地址”或“目标 MAC 地址”、“日志源”、“源 IPv6”或“目标 IPv6”、“源 ASN”或“目标 ASN”、“规则”或“应用程序标识”） • “排名前 5 位的源 IP”表 • “按源 IP 排列”详细信息页面 • “按目标 IP 排列 - 源列表”页面 • “按网络排列 - 源列表”页面 • “源详细信息”页面 • “排名前 5 位的目标 IP”表 • “按源 IP 排列 - 本地目标列表”页面 • “按目标 IP 排列”详细信息页面 • “按网络排列 - 本地目标列表”页面 • “排名前 5 位的用户”表 • “排名前 5 位的日志源”表 • “排名前 5 位的类别”表 • “按网络排列”详细信息页面 • “排名前 5 位的类别”表	指定与源 IP 地址、目标 IP 地址、事件名称、用户名、MAC 地址、日志源、主机名、端口、日志源、ASN 地址、IPv6 地址、规则、ASN、应用程序、网络或类别关联的事件或流数量。单击此链接可查看更多详细信息。
第一次遇到事件/流的时间	“源详细信息”页面	指定源 IP 地址生成第一个事件或流的日期和时间。

表 14. 攻击参数 (续)

参数	位置	描述
标志	• “所有攻击”页面 • “我的攻击”页面 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面	指示对攻击执行的操作。这些操作由下列图标表示: • 标志 - 指示已将攻击标记为需要跟进。这使您能够跟踪特定项以展开进一步调查。有关如何将攻击标记为需要跟进的更多信息，请参阅将项标记为需要跟进。 • 用户 - 指示已将攻击分配给用户。向用户分配攻击时，攻击将显示在属于该用户的“我的攻击”页面上。有关将攻击分配给用户的更多信息，请参阅将攻击分配给用户。 • 备注 - 指示用户已向攻击添加备注。备注可以包含任何要针对攻击捕获的信息。例如，可以添加备注来指定未自动包含在攻击中的信息，如客户支持凭单号或攻击管理信息。有关添加备注的更多信息，请参阅添加备注。 • 受保护 - 指示攻击受到保护。保护功能可以避免在保留期过后从数据库中除去指定的攻击。有关受保护的攻击的更多信息，请参阅保护攻击。 将鼠标悬停在此图标上方可显示更多信息。

表 14. 攻击参数 (续)

参数	位置	描述
标志（续）		• 处于非活动状态的攻击 - 指示这是处于非活动状态的攻击。自攻击接收到最后一个事件起 5 天后，攻击将变为非活动状态。另外，在升级 QRadar 产品软件后，所有攻击都将变为非活动状态。 处于非活动状态的攻击无法再次变为活动状态。如果检测到攻击的新事件，那么将创建新的攻击，并且处于非活动状态的攻击将一直保留到攻击保留期结束为止。您可以对处于非活动状态的攻击执行下列操作：保护、标记为需要跟进、添加备注以及分配给用户。
标志	• “按源 IP 排列”详细信息页面 • “按源 IP 排列 - 本地目标列表”页面 • “按目标 IP 排列”详细信息页面 • “按目标 IP 排列 - 源列表”页面 • “按网络排列”详细信息页面 • “按网络排列 - 源列表”页面 • “按网络排列 - 本地目标列表”页面	指定对源 IP 地址、目标 IP 地址或网络执行的操作。例如，如果显示了某个标志，那么标识该攻击标记为需要跟进。将鼠标悬停在此图标上方可显示更多信息。
流数量	• “所有攻击”页面 • “我的攻击”页面 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面	指定攻击的流数。 **注**：如果“流”列显示“不适用”，那么攻击的开始日期可能早于您升级到 QRadar 7.1.0 (MR1) 的日期。
组	• “攻击源”表（如果攻击类型是“日志源”） • “排名前 5 位的日志源”表	指定日志源所属的组。
组	“攻击源”表（如果攻击类型是“规则”）	指定规则所属的规则组。

表 14. 攻击参数 (续)

参数	位置	描述
高级别类别	“攻击源”表（如果攻击类型是“事件名称”）	指定事件的高级别类别。 有关高级别类别的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
主机名	“攻击源”表（如果攻击类型是“源 IP”或“目标 IP”）	指定与源或目标 IP 地址关联的主机名。如果未确定主机名，那么此字段指定“未知”。
历史关联概要文件名称	• 攻击摘要	指定创建攻击的历史关联概要文件的名称。
历史关联目录	• 攻击摘要	指定包含触发攻击的事件的历史关联目录。 要查看目录中的所有事件，请单击“历史关联”窗口上的**查看历史记录**。
历史关联概要文件标识	• 攻击摘要	指定创建攻击的历史关联概要文件的唯一标识。
主机名	“攻击源”表（如果攻击类型是“主机名”）	指定与创建攻击的流关联的主机名。
标识	• “所有攻击”页面 • “我的攻击”页面 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面	指定 QRadar 向攻击分配的唯一标识号。
IP	• “攻击源”表（如果攻击类型是“源 IP”或“目标 IP”） • “源详细信息”页面	指定与创建攻击的事件或流关联的源 IP 地址。
IP/DNS 名称	“目标”页面	指定目标的 IP 地址。如果在**管理**选项卡上启用了 DNS 查找，那么可以通过将鼠标悬停在 IP 地址或资产名称上方来查看 DNS 名称。 有关更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
IPv6	“攻击源”表（如果攻击类型是“源 IPv6”或“目标 IPv6”）	指定与创建攻击的事件或流关联的 IPv6 地址。

表 14. 攻击参数 (续)

参数	位置	描述
最后一个事件/流	• “所有攻击”页面 • “我的攻击”页面 • “按源 IP 排列 - 本地目标列表”页面 • “排名前 5 位的源 IP”表 • “按源 IP 排列”详细信息页面 • “按网络排列 - 源列表”页面 • “排名前 5 位的目标 IP”表 • “按目标 IP 排列”详细信息页面 • “按目标 IP 排列 - 源列表”页面 • “按网络排列 - 本地目标列表”页面 • “排名前 5 位的类别”表	指定针对攻击、类别、源 IP 地址或目标 IP 地址观察到最后一个事件或流以来经过的时间。
最近一次遇到事件/流的时间	“源详细信息”页面	指定与源 IP 地址关联的最近生成事件或流的日期和时间。
最后一个事件/流的时间	“攻击源”表（如果攻击类型是“日志源”）	指定最后在系统上观察到日志源的日期和时间。
最后一个已知的组	“攻击源”表（如果攻击类型是“用户名”、“源 MAC 地址”、“目标 MAC 地址”或“主机名”）	指定用户、MAC 地址或主机名当前所属的组。如果未关联任何组，那么此字段的值为“未知”。 **注**：此字段不会显示历史信息。
最后一个已知的主机	“攻击源”表（如果攻击类型是“用户名”、“源 MAC 地址”或“目标 MAC 地址”）	指定与用户或 MAC 地址关联的当前主机。如果未确定主机，那么此字段指定“未知”。 **注**：此字段不会显示历史信息。
最后一个已知的 IP	“攻击源”表（如果攻击类型是“用户名”、“源 MAC 地址”、“目标 MAC 地址”或“主机名”）	指定用户、MAC 或主机名的当前 IP 地址。如果未确定 IP 地址，那么此字段指定“未知”。 **注**：此字段不会显示历史信息。
最后一个已知的 MAC	“攻击源”表（如果攻击类型是“用户名”或“主机名”）	指定用户或主机名的最后一个已知的 MAC 地址。如果未确定 MAC，那么此字段指定“未知”。 **注**：此字段不会显示历史信息。

表 14. 攻击参数 (续)

参数	位置	描述
最后一个已知的机器	“攻击源”表（如果攻击类型是“用户名”、“源 MAC 地址”、“目标 MAC 地址”或“主机名”）	指定与用户、MAC 地址或主机名关联的当前机器名。如果未确定机器名，那么此字段指定“未知”。 **注**：此字段不会显示历史信息。
最后一个已知的用户名	“攻击源”表（如果攻击类型是“源 MAC 地址”、“目标 MAC 地址”或“主机名”）	指定 MAC 地址或主机名的当前用户。如果未确定 MAC 地址，那么此字段指定“未知”。 **注**：此字段不会显示历史信息。
最后观察时间	“攻击源”表（如果攻击类型是“用户名”、“源 MAC 地址”、“目标 MAC 地址”或“主机名”）	指定最后一次在系统中观察用户、MAC 地址或主机名的日期和时间。
最后一个包的时间	“最后 10 个流”表	指定流的最后一个包的发送日期和时间。
本地目标计数	“排名前 5 位的类别”表 “按类别排列”详细信息页面	指定与类别关联的本地目标 IP 地址数。
本地目标	“源详细信息”页面	指定与源 IP 地址关联的本地目标 IP 地址。要查看有关目标 IP 地址的更多信息，请单击显示的 IP 地址或词汇。 如果存在多个目标 IP 地址，那么将显示“多个”一词。
位置	• “攻击源”表（如果攻击类型是“源 IP”或“目标 IP”） • “排名前 5 位的源 IP”表 • “按源 IP 排列”详细信息页面 • “源详细信息”页面 • “按目标 IP 排列 - 源列表”页面 • “按网络排列 - 源列表”页面	指定源 IP 地址或目标 IP 地址的网络位置。如果此位置是本地位置，那么可以单击此链接来查看网络。
日志源	“最后 10 个事件”表	指定检测到事件的日志源。
日志源标识	“攻击源”表（如果攻击类型是“日志源”）	指定日志源的主机名。

表 14. 攻击参数 (续)

参数	位置	描述
日志源名称	“攻击源”表（如果攻击类型是“日志源”）	指定“日志源”表中标识的日志源名称，此名称与创建攻击的事件关联。 **注**：针对日志源攻击显示的信息派生自“管理”选项卡上的“日志源”页面。您必须具有管理访问权才能访问“管理”选项卡和管理日志源。有关日志源管理的更多信息，请参阅 *Managing Log Sources Guide*。
日志源	• “所有攻击”页面 • “我的攻击”页面 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面	指定与攻击关联的日志源。如果多个日志源与攻击关联，那么此字段指定“多个”以及日志源数量。
低级别类别	“攻击源”表（如果攻击类型是“事件名称”）	指定事件的低级别类别。
MAC	• “攻击源”表（如果攻击类型是“源 IP”或“目标 IP”） • “排名前 5 位的源 IP”表 • “排名前 5 位的目标 IP”表 • “按源 IP 排列”详细信息页面 • “按源 IP 排列 - 本地目标列表”页面 • “按目标 IP 排列”详细信息页面 • “按目标 IP 排列 - 源列表”页面 • “按网络排列 - 源列表”页面 • “按网络排列 - 本地目标列表”页面	指定攻击开始时源或目标 IP 地址的 MAC 地址。如果 MAC 地址未知，那么此字段指定“未知”。
MAC 地址	“攻击源”表（如果攻击类型是“源 MAC 地址”或“目标 MAC 地址”）	指定与创建攻击的事件关联的 MAC 地址。如果未确定 MAC 地址，那么此字段指定“未知”。

表 14. 攻击参数 (续)

参数	位置	描述
规模	• “所有攻击”页面 • “我的攻击”页面 • “攻击”表 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面 • “排名前 5 位的类别”表 • “最后 10 个事件”表 • “按网络排列”详细信息页面 • “网络”页面	指定攻击、类别、事件或网络的相对重要性。规模条提供所有关联变量的可视表示。这些变量包括“相关性”、“严重性”和“可信性”。将鼠标悬停在规模条上方可显示值和计算的规模。
规模	• “攻击源”表（如果攻击类型是“源 IP”或“目标 IP”） • “排名前 5 位的源 IP”表 • “排名前 5 位的目标 IP”表 • “按源 IP 排列”详细信息页面 • “源详细信息”页面 • “按源 IP 排列 - 本地目标列表”页面 • “目标”页面 • “按目标 IP 排列”详细信息页面 • “按目标 IP 排列 - 源列表”页面 • “按网络排列 - 源列表”页面 • “按网络排列 - 本地目标列表”页面	指定源或目标 IP 地址的相对重要性。规模条提供 IP 地址的关联资产 CVSS 风险值的可视表示。将鼠标悬停在规模条上方可显示计算的规模。
名称	• “排名前 5 位的日志源”表 • “排名前 5 位的用户”表 • “排名前 5 位的类别”表 • “网络”页面	指定日志源名称、用户、类别、网络 IP 地址或名称。
网络	“按网络排列”详细信息页面	指定网络的名称。
网络	“攻击”表	指定攻击的目标网络。如果攻击具有 1 个目标网络，那么此字段显示网络叶。单击此链接可查看网络信息。如果攻击具有多个目标网络，那么将显示“多个”一词。单击此链接可查看更多详细信息。

表 14. 攻击参数 (续)

参数	位置	描述
备注	• “攻击源”表（如果攻击类型是“规则”） • “最后 5 条备注”表	指定规则的备注。
攻击计数	“按类别排列”详细信息页面	指定每种类别的活动攻击数。活动攻击是指未隐藏或未关闭的攻击。 如果“按类别排列”详细信息页面包含“排除隐藏攻击”过滤器，那么“攻击计数”参数中显示的攻击计数可能不正确。如果要查看“按类别排列”窗格中的总计数，请单击“按类别排列”详细信息页面上“排除隐藏攻击”过滤器旁边的**清除过滤器**。
攻击源	• “所有攻击”页面 • “我的攻击”页面 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面	指定有关攻击源的信息。**攻击源**字段中显示的信息取决于攻击类型。例如，如果攻击类型是“源端口”，那么**攻击源**字段将显示创建攻击的事件的源端口。

表 14. 攻击参数 (续)

参数	位置	描述
攻击类型	• “我的攻击”页面 • “攻击”表 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面	指定攻击类型。攻击类型由创建攻击的规则确定。例如，如果攻击类型是“日志源事件”，那么生成攻击的规则会根据检测到事件的设备来关联事件。 攻击类型包括: • 源 IP • 目标 IP • 事件名称 • 用户名 • 源 MAC 地址 • 目标 MAC 地址 • 日志源 • 主机名 • 源端口 • 目标端口 • 源 IPv6 • 目标 IPv6 • 源 ASN • 目标 ASN • 规则 • 应用程序标识 攻击类型确定“攻击源摘要”窗格上显示的信息类型。
攻击	• “源详细信息”页面 • “目标”页面	指定与源或目标 IP 地址关联的攻击的名称。要查看有关攻击的更多信息，请单击显示的名称或词汇。 如果存在多个攻击，那么将显示“多个”一词。
已启动的攻击	“网络”页面	指定从网络启动的攻击。 如果存在多个此类攻击，那么此字段指定“多个”以及攻击数。
有目标的攻击	“网络”页面	指定针对网络的攻击。 如果存在多个此类攻击，那么此字段指定“多个”以及攻击数

表 14. 攻击参数 (续)

参数	位置	描述
攻击数	• “攻击源”表（如果攻击类型是“源 IP”、“目标 IP”、“事件名称”、“用户名”、“源 MAC 地址”或“目标 MAC 地址”、“日志源”、“主机名”、“源端口”或“目标端口”、“源 IPv6”或“目标 IPv6”、“源 ASN”或“目标 ASN”、“规则”或“应用程序标识”） • “排名前 5 位的源 IP”表 • “排名前 5 位的目标 IP”表 • “排名前 5 位的日志源”表 • “排名前 5 位的用户”表 • “按源 IP 排列”详细信息页面 • “按源 IP 排列 - 本地目标列表”页面 • “按目标 IP 排列”详细信息页面 • “按目标 IP 排列 - 源列表”页面 • “按网络排列 - 源列表”页面 • “按网络排列 - 本地目标列表”页面	指定与源 IP 地址、目标 IP 地址、事件名称、用户名、MAC 地址、日志源、主机名、端口、IPv6 地址、ASN、规则或应用程序关联的攻击数。单击此链接可查看更多详细信息。
已启动的攻击数	“按网络排列”详细信息页面	指定起源于网络的攻击数。
有目标的攻击数	“按网络排列”详细信息页面	指定针对网络的攻击数。
端口	“攻击源”表（如果攻击类型是“源端口”或“目标端口”）	指定与创建攻击的事件或流关联的端口。
相关性	“攻击”表	指定攻击的相对重要性。
响应	“攻击源”表（如果攻击类型是“规则”）	指定规则的响应类型。
规则描述	“攻击源”表（如果攻击类型是“规则”）	指定规则参数摘要。
规则名	“攻击源”表（如果攻击类型是“规则”）	指定与创建攻击的事件或流关联的规则名称。 **注**: 针对规则攻击显示的信息派生自**规则**选项卡。
规则类型	“攻击源”表（如果攻击类型是“规则”）	指定攻击的规则类型。

表 14. 攻击参数 (续)

参数	位置	描述
严重性	• “攻击源”表（如果攻击类型是“事件名称”） • “攻击”表	指定事件或攻击的严重性。严重性指示攻击所产生的威胁相对于目标 IP 地址应对攻击的准备情况的严重程度。此值直接映射到与攻击相关联的事件类别。例如，拒绝服务 (DoS) 攻击的严重性为 10，此值指定严重情况。
源计数	“按类别排列”详细信息页面	指定与类别中的攻击关联的源 IP 地址数。如果某个源 IP 地址与 5 个不同的低级别类别中的攻击关联，那么此源 IP 地址仅计算一次。
源 IP	• “按源 IP 排列”详细信息页面 • “按目标 IP 排列 - 源列表”页面 • “按网络排列 - 源列表”页面 • “排名前 5 位的源 IP”表 • “最后 10 个流”表	指定网络中尝试破坏组件安全性的设备的 IP 地址或主机名。如果在“管理”选项卡上启用了 DNS 查找，那么可以通过将鼠标悬停在 IP 地址上方来查看 DNS 名称。 有关更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
源 IP	“攻击”表	指定网络中尝试破坏组件安全性的设备的 IP 地址或主机名。单击此链接可查看更多详细信息。 有关源 IP 地址的更多信息，请参阅监视按源 IP 分组的攻击。
源 IP	• “所有攻击”页面 • “我的攻击”页面 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面	指定网络中尝试破坏组件安全性的设备的 IP 地址或主机名。如果多个源 IP 地址与攻击关联，那么此字段指定“多个”以及源 IP 地址数。如果在“管理”选项卡上启用了 DNS 查找，那么可以通过将鼠标悬停在 IP 地址或资产名称上方来查看 DNS 名称。 有关更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
源 IP 数	“按网络排列”详细信息页面	指定与网络关联的源 IP 地址的数量。
源端口	“最后 10 个流”表	指定流的源端口。

表 14. 攻击参数 (续)

参数	位置	描述
源数量	• “排名前 5 位的目标 IP”表 • “按源 IP 排列 - 本地目标列表”页面 • “按目标 IP 排列”详细信息页面	指定目标 IP 地址的源 IP 地址的数量。
源	• “目标”页面 • “网络”页面	指定与目标 IP 地址或网络关联的攻击的源 IP 地址。要查看有关源 IP 地址的更多信息，请单击显示的 IP 地址、资产名称或词汇。 如果指定了单个源 IP 地址，那么将显示一个 IP 地址和资产名称（如果可用）。单击此 IP 地址或资产名称可查看源 IP 地址详细信息。如果存在多个源 IP 地址，那么此字段指定“多个”以及源 IP 地址数。
源数量	“按网络排列 - 本地目标列表”页面	指定与目标 IP 地址关联的源 IP 地址的数量。
开始时间	“攻击”表	指定针对攻击第一次发生事件或流的日期和时间。
开始日期	• “所有攻击”页面 • “我的攻击”页面 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面	指定与攻击关联的第一个事件或流的日期和时间。
状态	“攻击源”表（如果攻击类型是“日志源”）	指定日志源的状态。

表 14. 攻击参数 (续)

参数	位置	描述
状态	“攻击”表	显示用于指示攻击状态的图标。状态图标包括: **处于非活动状态的攻击**。自攻击接收到最后一个事件起 5 天后，攻击将变为非活动状态。升级 QRadar 产品软件后，所有攻击都将变为非活动状态。 处于非活动状态的攻击无法再次变为活动状态。如果检测到攻击的新事件，那么将创建新的攻击，并且处于非活动状态的攻击将一直保留到攻击保留期结束为止。您可以对处于非活动状态的攻击执行保护、标记为需要跟进、添加备注以及分配给用户等操作。 “所有攻击”页面上的**隐藏的攻击**标志指示该攻击不可见。如果搜索隐藏的攻击，这些攻击仅在“所有攻击”页面上可见，并标记为隐藏的攻击。有关更多信息，请参阅隐藏攻击。 **用户**指示已将攻击分配给用户。向用户分配攻击时，攻击将显示在属于该用户的“我的攻击”页面上。有关更多信息，请参阅将攻击分配给用户。 **保护**可以避免在保留期过后从数据库中除去指定的攻击。有关更多信息，请参阅保护攻击。 **已关闭的攻击**指示攻击已关闭。有关更多信息，请参阅关闭攻击。
时间	• “最后 10 个事件”表 • “最后 10 个事件（异常事件）”表	指定在规范化事件中检测到第一个事件的日期和时间。此日期和时间由检测到事件的设备指定。
时间	“排名前 5 位的注释”表	指定注释的创建日期和时间。
总字节数	“最后 10 个流”表	指定流的总字节数。
事件/流总数	• “排名前 5 位的日志源”表 • “排名前 5 位的用户”表	指定日志源或用户的事件总数。

表 14. 攻击参数 (续)

参数	位置	描述
用户	• “攻击源”表（如果攻击类型是“源 IP”、“目标 IP”或“用户名”） • “排名前 5 位的源 IP”表 • “排名前 5 位的目标 IP”表 • “按源 IP 排列”详细信息页面 • “按源 IP 排列 - 本地目标列表”页面 • “按目标 IP 排列”详细信息页面 • “按目标 IP 排列 - 源列表”页面 • “按网络排列 - 源列表”页面 • “按网络排列 - 本地目标列表”页面	指定与源 IP 地址或目标 IP 地址关联的用户。如果未确定用户，那么此字段指定“未知”。
用户名	“攻击源”表（如果攻击类型是“用户名”）	指定与创建攻击的事件或流关联的用户名。 **注**：如果将鼠标指针移至“用户名”参数上方，将显示工具提示，其中提供与“资产”选项卡中最新用户名信息关联的用户名，而不是与创建攻击的事件或流关联的用户名。
用户名	“最后 5 条备注”表	指定创建备注的用户。
用户	• “所有攻击”页面 • “我的攻击”页面 • “按源 IP 排列 - 攻击列表”页面 • “按网络排列 - 攻击列表”页面 • “按目标 IP 排列 - 攻击列表”页面	指定与攻击关联的用户名。如果多个用户名与攻击相关联，那么此字段指定“多个”以及用户名数量。如果未确定用户，那么此字段指定“未知”。
查看攻击	• “按源 IP 排列”详细信息页面 • “按目标 IP 排列”详细信息页面	从该列表框中选择一个选项，以便对此页面上要查看的攻击进行过滤。您可以查看所有攻击，也可以基于时间范围对攻击进行过滤。从该列表框中，可以选择要作为过滤依据的时间范围。
漏洞数	“攻击源”表（如果攻击类型是“源 IP”或“目标 IP”）	指定与源或目标 IP 地址关联的已确定的漏洞数。此值还包括活动和被动漏洞数。

表 14. 攻击参数 (续)

参数	位置	描述
漏洞	“按目标 IP 排列 - 源列表”页面	指定源 IP 地址是否有漏洞。
漏洞	• “排名前 5 位的源 IP”表 • “按源 IP 排列”详细信息页面 • “按网络排列 - 源列表”页面 • “排名前 5 位的目标 IP”表 • “按源 IP 排列 - 本地目标列表”页面 • “按目标 IP 排列”详细信息页面 • “按网络排列 - 本地目标列表”页面	指定源 IP 地址或目标 IP 地址是否有漏洞。
权重	• “排名前 5 位的源 IP”表 • “排名前 5 位的目标 IP”表 • “按源 IP 排列 - 本地目标列表”页面 • “按源 IP 排列”详细信息页面 • “按目标 IP 排列”详细信息页面 • “按目标 IP 排列 - 源列表”页面 • “按网络排列 - 源列表”页面 • “按网络排列 - 本地目标列表”页面 • “排名前 5 位的注释”表	指定源 IP 地址、目标 IP 地址或注释的权重。IP 地址的权重在**资产**选项卡上指定。有关更多信息，请参阅资产管理。

第 5 章 日志活动调查

您可以实时地监视和调查事件或者执行高级搜索。

通过使用**日志活动**选项卡，您可以实时地监视和调查日志活动（事件）或者执行高级搜索。

“日志活动”选项卡概述

事件是来自日志源（例如防火墙或路由器设备）的记录，用于描述网络或主机中的操作。

日志活动选项卡指定了与攻击关联的事件。

您必须具有查看**日志活动**选项卡的许可权。

“日志活动”选项卡工具栏

您可以从“日志活动”工具栏访问多个选项

通过使用此工具栏，可以访问下列选项:

表 15. “日志活动”工具栏选项

选项	描述
搜索	单击**搜索**可以对事件执行高级搜索。 选项包括: • **新建搜索** - 选择此选项可以创建新的事件搜索。 • **编辑搜索** - 选择此选项可以选择并编辑事件搜索。 • **管理搜索结果** - 选择此选项可以查看和管理搜索结果。
快速搜索	从这个列表框中，可以运行先前保存的搜索。仅当已保存指定了**包括在快速搜索中**选项的搜索条件时，**快速搜索**列表框中才会显示选项。
添加过滤器	单击**添加过滤器**可以向当前搜索结果添加过滤器。
保存条件	单击**保存条件**可以保存当前搜索条件。
保存结果	单击**保存结果**可以保存当前搜索结果。只有在完成搜索后，才会显示此选项。在流方式下，此选项处于禁用状态。
取消	单击**取消**可以取消进行中的搜索。 在流方式下，此选项处于禁用状态。

表 15. “日志活动”工具栏选项 (续)

选项	描述
误报	单击**误报**将打开“误报调整”窗口，此窗口允许您阻止已确定为误报的事件创建攻击。 在流方式下，此选项处于禁用状态。有关调整误报的更多信息，请参阅调整误报。
规则	仅当您有权查看规则时，才会显示“规则”选项。 单击**规则**可以配置定制事件规则。 选项包括: • **规则** - 选择此选项可以查看或创建规则。如果您仅有权查看规则，那么将显示“规则”向导的摘要页面。 如果您有权维护定制规则，那么将显示“规则”向导，并且您可以编辑规则。 要启用异常检测规则选项（“添加阈值规则”、“添加行为规则”和“添加异常规则”），您必须保存汇总搜索条件，这是因为保存的搜索条件指定了必需的参数。 **注**: 仅当您具有**日志活动 > 维护定制规则**许可权时，才会显示异常检测规则选项。 • **添加阈值规则** - 选择此选项可以创建阈值规则。 阈值规则对事件流量进行测试，以查找超出了所配置阈值的活动。 阈值可以基于 QRadar 所收集的任何数据。例如，如果您创建了一条阈值规则，指出上午 8 点到下午 5 点之间不得有 220 个以上的客户机登录服务器，那么在第 221 个客户机尝试登录时，此规则将生成警报。 如果选择了**添加阈值规则**选项，那么将显示“规则”向导，其中预先填充了用于创建阈值规则的相应选项。

表 15. “日志活动”工具栏选项 (续)

选项	描述
规则（续）	• **添加行为规则** - 选择此选项可以创建行为规则。 行为规则对事件流量进行测试以识别异常活动，例如存在新流量或未知流量（突然停止的流量，或者对象处于活动状态的时间百分比发生变化的流量）。例如，您可以创建一条行为规则，用于将过去 5 分钟的平均流量与过去一小时的平均流量进行比较。如果变化幅度超过 40%，那么此规则将生成响应。 如果选择了**添加行为规则**选项，那么将显示“规则”向导，其中预先填充了用于创建行为规则的相应选项。 • **添加异常规则** - 选择此选项可以创建异常规则。 异常规则对事件流量进行测试以识别异常活动，例如存在新流量或未知流量（突然停止的流量，或者对象处于活动状态的时间百分比发生变化的流量）。例如，如果某个从未与亚洲进行通信的网络区域开始与该地区的主机进行通信，那么异常规则将生成警报。 如果选择了**添加异常规则**选项，那么将显示“规则”向导，其中预先填充了用于创建异常规则的相应选项。

表 15. “日志活动”工具栏选项 (续)

选项	描述
操作	单击**操作**可以执行下列操作: • **全部显示** - 选择此选项可以除去所有对搜索条件应用的过滤器，并显示所有事件（未进行过滤）。 • **打印** - 选择此选项可以打印页面上显示的事件。 • **导出为 XML > 可见列** - 选择此选项将仅导出“日志活动”选项卡上可见的列。 建议使用此选项。 请参阅『导出事件』。 • **导出为 XML > 完全导出（所有列）** - 选择此选项将导出所有事件参数。 完全导出可能需要较长时间才能完成。请参阅导出事件。 • **导出为 CSV > 可见列** - 选择此选项将仅导出“日志活动”选项卡上可见的列。 建议使用此选项。 请参阅导出事件。 • **导出为 CSV > 完全导出（所有列）** - 选择此选项将导出所有事件参数。 完全导出可能需要较长时间才能完成。请参阅导出事件。 • **删除** - 选择此选项可以删除搜索结果。 请参阅管理事件和流搜索结果。 • **通知** - 选择此选项可以指定您希望所选搜索完成时通过电子邮件向您发送通知。 仅对于进行中的搜索才会启用此选项。 **注**: 在流方式下，以及在查看不完整的搜索结果时，**打印**、**导出为 XML** 和**导出为 CSV** 选项处于禁用状态。
搜索工具栏	**高级搜索** 从列表框中选择**高级搜索**，以输入 Ariel Query Language (AQL) 搜索字符串来指定您希望返回的字段。 **快速过滤** 从列表框中选择“快速过滤”以便使用简单字或短语来搜索有效内容。
视图	**日志活动**选项卡上的缺省视图是实时事件流。**视图**列表包含一些选项，也可以用于查看指定时间段内的事件。从**视图**列表中选择指定时间段后，您可以通过更改**开始时间**和**结束时间**字段中的日期和时间值来修改所显示的时间段。

右键单击菜单选项

在**日志活动**选项卡上，可以右键单击事件以访问更多事件过滤器信息。

右键单击菜单选项如下:

表 16. 右键单击菜单选项

选项	描述
过滤	选择此选项可以按选择的事件进行过滤，具体取决于该事件中的选定参数。
误报	选择此选项将打开“误报”窗口，此窗口允许您阻止已知是误报的事件创建攻击。 在流方式下，此选项处于禁用状态。请参阅调整误报。
更多选项:	选择此选项可以调查 IP 地址或用户名。 有关调查 IP 地址的更多信息，请参阅“调查 IP 地址”。 有关调查用户名的更多信息，请参阅调查用户名。 **注**: 在流方式下，不会显示此选项。
快速过滤	与所选项匹配或不匹配的过滤器项。

状态栏

对事件执行流式方法处理时，状态栏将显示每秒接收到的平均结果数。

这是控制台从事件处理器成功接收到的结果数。 如果此数目大于每秒 40 个结果，那么将仅显示 40 个结果。 其余的项将在结果缓冲区中累积。 要查看更多状态信息，请将鼠标指针移动到状态栏上。

未对事件执行流式方式处理时，状态栏将显示选项卡上当前显示的搜索结果数，以及处理搜索结果所需的时间长度。

日志活动监视

缺省情况下，**日志活动**选项卡以流方式显示事件，这使您能够实时查看事件。

有关流方式的更多信息，请参阅查看流式事件。 您可以使用**查看**列表框来指定另一时间范围，以便对事件进行过滤。

如果您先前已将某个已保存的搜索条件配置为缺省条件，那么您访问**日志活动**选项卡时，会自动显示该搜索的结果。有关保存搜索条件的更多信息，请参阅保存事件和流搜索条件。

查看流式事件

流方式将使您能够查看进入系统的事件数据。 此方式通过显示最近 50 个事件为您提供有关当前事件活动的实时视图。

关于此任务

如果在启用流方式之前在**日志活动**选项卡或搜索条件中应用了任何过滤器，那么这些过滤器将在流方式下进行维护。 但是，流方式不支持包含已分组事件的搜索。 如果对已分组事件或已分组搜索条件启用流方式，那么**日志活动**选项卡将显示规范化事件。 请参阅查看规范化事件。

如果要选择一个事件以查看详细信息或执行操作，那么必须先暂停流式方法，然后再双击一个事件。 暂停流式方法后，将显示最近 1,000 个事件。

过程

1. 单击**日志活动**选项卡。
2. 从**视图**列表框中，选择**实时（流式方法）**。 有关工具栏选项的信息，请参阅表 4-1。有关流方式下显示的参数的更多信息，请参阅表 4-7。
3. 可选。 暂停或启动流式事件。 选择下列其中一个选项:
   - 要选择事件记录，请单击**暂停**图标以暂停流式方法。
   - 要重新启动流方式，请单击**启动**图标。

查看规范化事件

事件以原始格式进行收集，然后进行规范化以便显示在**日志活动**选项卡中。

关于此任务

规范化涉及解析原始事件数据，以及准备此数据以便显示有关选项卡的可读信息。 对事件进行规范化时，系统还会对名称进行规范化。 因此，**日志活动**选项卡中显示的名称可能与事件中显示的名称不匹配。

注: 如果选择了要显示的时间范围，那么将显示一个时间序列图表。有关使用时间序列图表的更多信息，请参阅时间序列图表概述。

查看规范化事件时，**日志活动**选项卡将显示下列参数:

表 17. "日志活动"选项卡 - 缺省值（规范化）参数

参数	描述
当前过滤器	表顶部显示应用于搜索结果的过滤器的详细信息。 要清除这些过滤器值，请单击**清除过滤器**。 **注:** 仅当您应用过滤器后，才会显示此参数。
视图	从此列表框中，可以选择要过滤的时间范围。
当前的统计信息	在"实时（流式方法）"或"上一分钟（自动刷新）"方式以外的方式下，将显示当前统计信息，其中包括: **注:** 单击**当前统计信息**旁边的箭头可以显示或隐藏统计信息。 • **总结果数** - 指定满足搜索条件的结果总数。 • **搜索到的数据文件数** - 指定在指定的时间范围内搜索到的数据文件总数。 • **搜索到的压缩数据文件数** - 指定在指定的时间范围内搜索到的压缩数据文件总数。 • **索引文件计数** - 指定在指定的时间范围内搜索到的索引文件总数。 • **持续时间** - 指定搜索的持续时间。 **注:** 当前统计信息对于故障诊断而言非常有用。 联系客户支持以便对事件进行故障诊断时，可能会要求您提供当前统计信息。

表 17. “日志活动”选项卡 - 缺省值（规范化）参数 (续)

参数	描述
图表	显示可配置图表，这些图表表示与时间间隔和分组选项相匹配的记录。如果不希望显示图表，请单击**隐藏图表**。仅当您选择上次时间间隔（自动刷新）或更广的时间范围，并且选择要显示的分组选项后，才会显示图表。有关配置图表的更多信息，请参阅图表管理。 **注**：如果您使用 Mozilla Firefox 作为浏览器，并且安装了广告拦截器浏览器扩展，那么图表无法显示。要显示图表，必须除去广告拦截器浏览器扩展。有关更多信息，请参阅浏览器文档。
“攻击”图标	单击此图标可以显示与此事件相关联的攻击的详细信息。有关更多信息，请参阅图表管理。 **注**：根据您的产品不同，此图标可能会不可用。您必须具有 IBM Security QRadar SIEM。
开始时间	指定日志源向 QRadar 报告第一个事件的时间。
事件名称	指定事件的规范化名称。
日志源	指定发起事件的日志源。如果存在多个与此事件相关联的日志源，那么此字段将显示“多个”一词以及日志源数。
事件计数	指定此规范化事件中捆绑的事件总数。在短时间内检测到同一个源和目标 IP 地址的许多同一类事件时，这些事件将进行捆绑。
时间	指定 QRadar 接收到事件的日期和时间。
低级别类别	指定与此事件相关联的低级别类别。 有关事件类别的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
源 IP	指定此事件的源 IP 地址。
源端口	指定此事件的源端口。
目标 IP	指定此事件的目标 IP 地址。
目标端口	指定此事件的目标端口。
用户名	指定与此事件相关联的用户名。用户名通常在与认证相关的事件中提供。对于所有其他未提供用户名的事件类型，此字段指定“不适用”。
规模	指定此事件的规模。变量包括可信性、相关性和严重性。将鼠标悬停在规模条上方可显示值和计算的规模。

过程

1. 单击**日志活动**选项卡。
2. 从**显示**列表框中，选择**缺省值（规范化）**。
3. 从**视图**列表框中，选择要显示的时间范围。
4. 单击**暂停**图标以暂停流式方法。

5. 双击要查看其详细信息的事件。 有关更多信息，请参阅事件详细信息。

查看原始事件

您可以查看原始事件数据，即，日志源中未解析的事件数据。

关于此任务

查看原始事件数据时，**日志活动**选项卡提供了各个事件的下列参数。

表 18. 原始事件参数

参数	描述
当前过滤器	表顶部显示应用于搜索结果的过滤器的详细信息。 要清除这些过滤器值，请单击**清除过滤器**。 **注:** 仅当您应用过滤器后，才会显示此参数。
视图	从此列表框中，可以选择要过滤的时间范围。
当前统计信息	在“实时（流式方法）”或“上一分钟（自动刷新）”方式以外的方式下，将显示当前统计信息，其中包括: **注:** 单击**当前统计信息**旁边的箭头可以显示或隐藏统计信息。 • **总结果数** - 指定满足搜索条件的结果总数。 • **搜索到的数据文件数** - 指定在指定的时间范围内搜索到的数据文件总数。 • **搜索到的压缩数据文件数** - 指定在指定的时间范围内搜索到的压缩数据文件总数。 • **索引文件计数** - 指定在指定的时间范围内搜索到的索引文件总数。 • **持续时间** - 指定搜索的持续时间。 **注:** 当前统计信息对于故障诊断而言非常有用。 联系客户支持以便对事件进行故障诊断时，可能会要求您提供当前统计信息。
图表	显示可配置图表，这些图表表示与时间间隔和分组选项相匹配的记录。 如果不希望显示图表，请单击**隐藏图表**。 仅当您选择上次时间间隔（自动刷新）或更广的时间范围，并且选择要显示的分组选项后，才会显示图表。 **注:** 如果您使用 Mozilla Firefox 作为浏览器，并且安装了广告拦截器浏览器扩展，那么图表无法显示。要显示图表，必须除去广告拦截器浏览器扩展。有关更多信息，请参阅浏览器文档。
“攻击”图标	单击此图标可以显示与此事件相关联的攻击的详细信息。
开始时间	指定日志源向 QRadar 报告第一个事件的时间。
日志源	指定发起事件的日志源。 如果存在多个与此事件相关联的日志源，那么此字段将显示“多个”一词以及日志源数。

表 18. 原始事件参数 (续)

参数	描述
有效内容	以 UTF-8 格式指定原始事件有效内容信息。

过程

1. 单击**日志活动**选项卡。
2. 从**显示**列表框中，选择**原始事件**。
3. 从**视图**列表框中，选择要显示的时间范围。
4. 双击要查看其详细信息的事件。 请参阅事件详细信息。

查看已分组的事件

通过使用**日志活动**选项卡，您可以查看按各个选项进行了分组的事件。 您可以从**显示**列表框中选择要作为事件分组依据的参数。

关于此任务

流方式不支持已分组的事件，因此，在流方式下“显示”列表框不会显示。 如果您使用不分组搜索条件进入了流方式，那么将显示此选项。

“显示”列表框提供了下列选项:

表 19. 分组事件选项

组选项	描述
低级别类别	显示按事件的低级别类别分组的事件的汇总列表。 有关类别的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
事件名称	显示按事件的规范化名称分组的事件的汇总列表。
目标 IP	显示按事件的目标 IP 地址分组的事件的汇总列表。
目标端口	显示按事件的目标端口地址分组的事件的汇总列表。
源 IP	显示按事件的源 IP 地址分组的事件的汇总列表。
定制规则	显示按关联的定制规则分组的事件的汇总列表。
用户名	显示按与事件相关联的用户名分组的事件的汇总列表。
日志源	显示按向 QRadar 发送事件的日志源分组的事件的汇总列表。
高级别类别	显示按事件的高级别类别分组的事件的汇总列表。
网络	显示按与事件相关联的网络分组的事件的汇总列表。

表 19. 分组事件选项 (续)

组选项	描述
源端口	显示按事件的源端口地址分组的事件的汇总列表。

从**显示**列表框中选择一个选项后，数据的列布局将取决于所选组选项。事件表中的每行都表示一个事件组。 **日志活动**选项卡提供了各个事件组的以下信息:

表 20. 分组事件参数

参数	描述
分组依据	指定作为搜索分组依据的参数。
当前过滤器	表顶部显示应用于搜索结果的过滤器的详细信息。 要清除这些过滤器值，请单击**清除过滤器**。
视图	从列表框中，选择要过滤的时间范围。
当前统计信息	在“实时（流式方法）”或“上一分钟（自动刷新）”方式以外的方式下，将显示当前统计信息，其中包括: **注**: 单击**当前统计信息**旁边的箭头可以显示或隐藏统计信息。 • **总结果数** - 指定满足搜索条件的结果总数。 • **搜索到的数据文件数** - 指定在指定的时间范围内搜索到的数据文件总数。 • **搜索到的压缩数据文件数** - 指定在指定的时间范围内搜索到的压缩数据文件总数。 • **索引文件计数** - 指定在指定的时间范围内搜索到的索引文件总数。 • **持续时间** - 指定搜索的持续时间。 **注**: 当前统计信息对于故障诊断而言非常有用。 联系客户支持以便对事件进行故障诊断时，可能会要求您提供当前统计信息。

表 20. 分组事件参数 (续)

参数	描述
图表	显示可配置图表，这些图表表示与时间间隔和分组选项相匹配的记录。如果不希望显示图表，请单击**隐藏图表**。 每个图表都提供了图注，后者是一个可视参考，用于帮助您使图表对象与其表示的参数相关联。 通过使用图注功能部件，可以执行下列操作: • 将鼠标指针移到图注项上方，以查看更多关于所表示的参数的信息。 • 右键单击图注项，以便对该项进行进一步调查。 • 单击图注项，以便在图表中隐藏该项。 再次单击该图注项将显示隐藏的项。 您也可以单击相应的图形项以隐藏和显示该项。 • 如果要从图表显示中除去图注，请单击**图注**。 **注**: 仅当您选择上次时间间隔（自动刷新）或更广的时间范围，并且选择要显示的分组选项后，才会显示图表。 **注**: 如果您使用 Mozilla Firefox 作为浏览器，并且安装了广告拦截器浏览器扩展，那么图表无法显示。要显示图表，必须除去广告拦截器浏览器扩展。有关更多信息，请参阅浏览器文档。
源 IP（唯一计数）	指定与此事件相关联的源 IP 地址。 如果存在多个与此事件相关联的 IP 地址，那么此字段将显示“多个”一词以及 IP 地址数。
目标 IP（唯一计数）	指定与此事件相关联的目标 IP 地址。 如果存在多个与此事件相关联的 IP 地址，那么此字段将显示“多个”一词以及 IP 地址数。
目标端口（唯一计数）	指定与此事件相关联的目标端口。 如果存在多个与此事件相关联的端口，那么此字段将显示“多个”一词以及端口数。
事件名称	指定事件的规范化名称。
日志源（唯一计数）	指定将事件发送到 QRadar 的日志源。如果存在多个与此事件相关联的日志源，那么此字段将显示“多个”一词以及日志源数。
高级别类别（唯一计数）	指定此事件的高级别类别。 如果存在多个与此事件相关联的类别，那么此字段将显示“多个”一词以及类别数。 有关类别的更多信息，请参阅 *IBM Security QRadar Log Manager Administration Guide*。
低级别类别（唯一计数）	指定此事件的低级别类别。 如果存在多个与此事件相关联的类别，那么此字段将显示“多个”一词以及类别数。

表 20. 分组事件参数 (续)

参数	描述
协议（唯一计数）	指定与此事件相关联的协议标识。 如果存在多个与此事件相关联的协议，那么此字段将显示“多个”一词以及协议标识数。
用户名（唯一计数）	指定与此事件相关联的用户名（如果有）。 如果存在多个与此事件相关联的用户名，那么此字段将显示“多个”一词以及用户名数。
规模（最大值）	指定已分组事件的最大计算规模。 用于计算规模的变量包括可信性、相关性和严重性。 有关可信性、相关性和严重性的更多信息，请参阅词汇表。
事件计数（总和）	指定此规范化事件中捆绑的事件总数。 在短时间内检测到同一个源和目标 IP 地址的许多同一类事件时，这些事件将进行捆绑。
计数	指定此事件组中的规范化事件数。

过程

1. 单击**日志活动**选项卡。
2. 从**视图**列表框中，选择要显示的时间范围。
3. 从“显示”列表框中，选择要作为事件分组依据的参数。 请参阅表 2。 列出了事件组。有关事件组详细信息的更多信息， 请参阅表 1。
4. 要查看某个组的“事件列表”页面，请双击要调查的事件组。 “事件列表”页面未保留您可能已在**日志活动**选项卡中定义的图表配置。有关“事件列表”页面的更多信息，请参阅表 1。
5. 要查看某个事件的详细信息，请双击要调查的事件。 有关事件详细信息的更多信息，请参阅表 2。

事件详细信息

您可以通过各种方式（包括流方式或事件组方式）查看事件列表。 无论您选择以何种方式查看事件，都可以查找并查看单个事件的详细信息。

事件详细信息页面提供了以下信息:

表 21. 事件详细信息

参数	描述
事件名称	指定此事件的规范化名称。
低级别类别	指定此事件的低级别类别。 有关类别的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
事件描述	指定此事件的描述（如果有）。
规模	指定此事件的规模。 有关规模的更多信息，请参阅词汇表
相关性	指定此事件的相关性。 有关相关性的更多信息，请参阅词汇表。

表 21. 事件详细信息 (续)

参数	描述
严重性	指定此事件的严重性。 有关严重性的更多信息，请参阅词汇表。
可信性	指定此事件的可信性。 有关可信性的更多信息，请参阅词汇表。
用户名	指定与此事件关联的用户名（如果有）。
开始时间	指定从日志源接收到事件的时间。
存储时间	指定将事件存储到 QRadar 数据库的时间。
日志源时间	指定日志源在事件有效内容中报告的系统时间。
异常检测信息 - 仅当此事件由异常检测规则生成时，才会显示此窗格。 单击**异常**图标可以查看导致异常检测规则生成此事件的已保存搜索结果。	
规则描述	指定生成了此事件的异常检测规则。
异常描述	指定对异常检测规则所检测到的异常行为的描述。
异常警报值	指定异常警报值。
源及目标信息	
源 IP	指定此事件的源 IP 地址。
目标 IP	指定此事件的目标 IP 地址。
源资产名称	指定事件源的用户定义资产名称。 有关资产的更多信息，请参阅『资产管理』。
目标资产名称	指定事件目标的用户定义资产名称。 有关资产的更多信息，请参阅『资产管理』
源端口	指定此事件的源端口。
目标端口	指定此事件的目标端口。
NAT 前的源 IP	对于防火墙或者其他具有网络地址转换 (NAT) 功能的设备，此参数指定应用 NAT 值之前的源 IP 地址。 NAT 用于将一个网络中的 IP 地址转换为另一网络中的其他 IP 地址。
NAT 前的目标 IP	对于防火墙或者其他具有 NAT 功能的设备，此参数指定应用 NAT 值之前的目标 IP 地址。
NAT 前的源端口	对于防火墙或者其他具有 NAT 功能的设备，此参数指定应用 NAT 值之前的源端口。
NAT 前的目标端口	对于防火墙或者其他具有 NAT 功能的设备，此参数指定应用 NAT 值之前的目标端口。
NAT 后的源 IP	对于防火墙或者其他具有 NAT 功能的设备，此参数指定应用 NAT 值之后的源 IP 地址。
NAT 后的目标 IP	对于防火墙或者其他具有 NAT 功能的设备，此参数指定应用 NAT 值之后的目标 IP 地址。
NAT 后的源端口	对于防火墙或者其他具有 NAT 功能的设备，此参数指定应用 NAT 值之后的源端口。
NAT 后的目标端口	对于防火墙或者其他具有 NAT 功能的设备，此参数指定应用 NAT 值之后的目标端口。

表 21. 事件详细信息 (续)

参数	描述
NAT 后的源端口	对于防火墙或者其他具有 NAT 功能的设备，此参数指定应用 NAT 值之后的源端口。
NAT 后的目标端口	对于防火墙或者其他具有 NAT 功能的设备，此参数指定应用 NAT 值之后的目标端口。
IPv6 源	指定此事件的源 IPv6 地址。
IPv6 目标	指定此事件的目标 IPv6 地址。
源 MAC	指定此事件的源 MAC 地址。
目标 MAC	指定此事件的目标 MAC 地址。
有效内容信息	
有效内容	指定此事件中的有效内容。此字段提供了 3 个选项卡，用于查看有效内容: • 通用转换格式 (UTF) - 请单击 UTF。 • 十六进制 - 请单击 HEX。 • Base64 - 请单击 Base64。
其他信息	
协议	指定与此事件关联的协议。
QID	指定此事件的 QID。 每个事件都具有唯一的 QID。 有关映射 QID 的更多信息，请参阅修改事件映射。
日志源	指定将事件发送到 QRadar 的日志源。如果存在多个与此事件关联的日志源，那么此字段将显示“多个”一词以及日志源数量。
事件计数	指定此规范化事件中捆绑的事件总数。 在短时间内检测到同一个源和目标 IP 地址的许多同一类型事件时，这些事件将进行捆绑。
定制规则	指定与此事件匹配的定制规则。 .
部分匹配的定制规则	指定与此事件部分匹配的定制规则。
注释	指定此事件的注释。 注释是规则可以对事件自动添加的文本描述，作为规则响应的组成部分。
身份信息 - QRadar 从日志源消息中收集身份信息（如果有）。 身份信息提供有关网络中的资产的额外详细信息。 仅当发送到 QRadar 的日志消息包含 IP 地址以及至少下列其中一项内容时，日志源才会生成身份信息: 用户名或 MAC 地址。 并非所有日志源都会生成身份信息。 有关身份和资产的更多信息，请参阅资产管理。	
身份用户名	指定与此事件关联的资产的用户名。
身份 IP	指定与此事件关联的资产的 IP 地址。
身份 Net Bios 名称	指定与此事件关联的资产的网络基本输入/输出系统 (Net Bios) 名称。
扩展身份字段	指定与此事件关联的资产的更多相关信息。 此字段的内容是用户定义的文本，并且依赖于网络中可用于提供身份信息的设备。 示例包括: 设备的物理位置、相关策略、网络交换机和端口名称。

表 21. 事件详细信息 (续)

参数	描述
具有身份（标志）	如果 QRadar 已收集与此事件关联的资产的身份信息，那么此参数将指定 True。 有关哪些设备发送身份信息的更多信息，请参阅 *IBM Security QRadar DSM Configuration Guide*。
身份主机名	指定与此事件关联的资产的主机名。
身份 MAC	指定与此事件关联的资产的 MAC 地址。
身份组名	指定与此事件关联的资产的组名。

“事件详细信息”工具栏

“事件详细信息”工具栏提供了多项用于查看事件详细信息的功能。

事件详细信息工具栏提供了下列功能:

表 22. “事件详细信息”工具栏

返回到事件列表	单击**返回到事件列表**可以返回到事件列表。
攻击	单击**攻击**可以显示与事件关联的攻击。
异常	单击**异常**可以显示导致异常检测规则生成此事件的已保存搜索结果。 **注**: 仅当此事件由异常检测规则生成时，才会显示此图标。
映射事件	单击**映射事件**可以对事件映射进行编辑。 有关更多信息，请参阅修改事件映射。
误报	单击**误报**可调整 QRadar，以防止在攻击中生成误报事件。
抽取属性	单击**抽取属性**可以根据选择的事件创建定制事件属性。
上一个	单击**上一个**可以查看事件列表中的上一个事件。
下一个	单击**下一个**可以查看事件列表中的下一个事件。
PCAP 数据	**注**: 仅当 QRadar 控制台配置为与 Juniper JunOS Platform DSM 集成时，才会显示此选项。有关管理 PCAP 数据的更多信息，请参阅管理 PCAP 数据。 • **查看 PCAP 信息** - 选择此选项可查看 PCAP 信息。有关更多信息，请参阅查看 PCAP 信息。 • **下载 PCAP 文件** - 选择此选项可以将 PCAP 文件下载到桌面系统。有关更多信息，请参阅将 PCAP 文件下载到桌面系统。
打印	单击**打印**可以打印事件详细信息。

查看相关联的攻击

您可以通过“日志活动”选项卡查看与事件相关联的攻击。

关于此任务

如果事件与规则匹配，那么可以在**攻击**选项卡上生成攻击。

有关规则的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

通过**日志活动**选项卡查看攻击时，如果 Magistrate 尚未将与所选事件相关联的攻击保存到磁盘或者此攻击已从数据库中清除，那么可能不会显示此攻击。 如果发生这种情况，那么系统将向您发送通知。

过程

1. 单击**日志活动**选项卡。
2. 可选。 如果您是以流方式查看事件，请单击**暂停**图标以暂停流。
3. 单击要调查的事件旁边的**攻击**图标。
4. 查看相关联的攻击。

修改事件映射

可以将规范化事件或原始事件手动映射到高级别类别和低级别类别（或者 QID）。

开始之前

此手动操作用于将未知的日志源事件映射到已知的 QRadar 事件，以便适当地对这些未知事件进行分类和处理。

关于此任务

为了进行规范化，QRadar 将来自日志源的事件自动映射到高级别类别和低级别类别。

有关事件类别的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

如果从日志源接收到系统无法进行分类的事件，那么这些事件将归类为未知事件。这些事件由于多种原因而发生，其中包括:

- **用户定义的事件** - 某些日志源（例如 Snort）允许您创建用户定义的事件。
- **新事件或旧事件** - 供应商日志源可能通过维护版更新其软件，以支持 QRadar 可能不支持的新事件。

注: 高级别类别为“SIM 审计”或者日志源类型为简单对象访问协议 (SOAP) 时，**映射事件**图标对事件处于禁用状态。

过程

1. 单击**日志活动**选项卡。
2. 可选。 如果您是以流方式查看事件，请单击**暂停**图标以暂停流。
3. 双击要映射的事件。
4. 单击**映射事件**。
5. 如果您知道要将此事件映射到的 QID，请在**输入 QID** 字段中输入此 QID。

6. 如果您不知道要将此事件映射到的 QID，那么可以搜索特定 QID:
   a. 选择下列其中一个选项: 要按类别搜索 QID，请从"高级别类别"列表框中选择高级别类别。 要按类别搜索 QID，请从"低级别类别"列表框中选择低级别类别。 要按日志源类型搜索 QID，请从"日志源类型"列表框中选择日志源类型。 要按名称搜索 QID，请在"QID/名称"字段中输入名称。
   b. 单击**搜索**。
   c. 选择要与此事件相关联的 **QID**。
7. 单击**确定**。

调整误报

使用“误报调整”功能可以阻止误报事件创建攻击。

开始之前

您可以从“事件列表”或“事件详细信息”页面调整误报事件。

关于此任务

您可以从“事件列表”或“事件详细信息”页面调整误报事件。

您必须具有创建定制规则的相应许可权才能调整误报。

有关角色的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

有关误报的更多信息，请参阅词汇表。

过程

1. 单击**日志活动**选项卡。
2. 可选。 如果您是以流方式查看事件，请单击**暂停**图标以暂停流。
3. 选择要调整的事件。
4. 单击**误报**。
5. 在“误报”窗口上的“事件/流属性”窗格中，选择下列其中一个选项:
   - 具有特定 QID <Event> 的事件/流
   - 任何具有低级别类别 <Event> 的事件/流
   - 任何具有高级别类别 <Event> 的事件/流
6. 在“流量方向”窗格中，选择下列其中一个选项:
   - <源 IP 地址> 到 <目标 IP 地址>
   - <源 IP 地址> 到任何目标
   - 任何源到 <目标 IP 地址>
   - 任何源到任何目标
7. 单击**调整**。

PCAP 数据

如果 QRadar 控制台配置为与 Juniper JunOS Platform DSM 集成，那么可以接收、处理和存储来自 Juniper SRX 系列服务网关日志源的包捕获 (PCAP) 数据。

有关 Juniper JunOS Platform DSM 的更多信息，请参阅 *IBM Security QRadar DSM Configuration Guide*。

显示 PCAP 数据列

缺省情况下，**日志活动**选项卡未显示 **PCAP 数据**列。 创建搜索条件时，必须在“列定义”窗格中选择 **PCAP 数据**列。

开始之前

必须先将 Juniper SRX 系列服务网关日志源配置为使用 PCAP 系统日志组合协议，然后才能在**日志活动**选项卡上显示 PCAP 数据。 有关配置日志源协议的更多信息，请参阅 *Managing Log Sources Guide*。

关于此任务

执行包含 **PCAP 数据**列的搜索时，如果可以获得事件的 PCAP 数据，那么搜索结果的 **PCAP 数据**列将显示一个图标。 通过使用 **PCAP** 图标，您可以查看 PCAP 数据或者将 **PCAP** 文件下载到桌面系统。

过程

1. 单击**日志活动**选项卡。
2. 从**搜索**列表框中，选择**新建搜索**。
3. 可选。 要搜索具有 PCAP 数据的事件，请配置以下搜索条件:
   a. 从第一个列表框中，选择 **PCAP 数据**。
   b. 从第二个列表框中，选择**等于**。
   c. 从第三个列表框中，选择 **True**。
   d. 单击**添加过滤器**。
4. 将列定义配置为包括 **PCAP 数据**列:
   a. 从“列定义”窗格的**可用列**列表中，单击 **PCAP 数据**。
   b. 单击底部图标集中的**添加列**图标，以便将 **PCAP 数据**列移至**列**列表。
   c. 可选。 单击顶部图标集中的**添加列**图标，以便将 **PCAP 数据**列移至**分组依据**列表。
5. 单击**过滤**。
6. 可选。 如果您是以流方式查看事件，请单击**暂停**图标以暂停流。
7. 双击要调查的事件。

下一步做什么

有关查看和下载 PCAP 数据的更多信息，请参阅下列各节:

- 查看 PCAP 信息
- 将 PCAP 文件下载到桌面系统

查看 PCAP 信息

通过 **PCAP 数据**工具栏菜单，您可以查看 PCAP 文件中数据的可读版本，或者将 PCAP 文件下载到桌面系统。

开始之前

必须先执行或选择显示了 **PCAP 数据**列的搜索，然后才能查看 PCAP 信息。

关于此任务

必须先检索 PCAP 文件以将其显示在用户界面上，然后才能显示 PCAP 数据。 如果下载过程所用的时间较长，那么将显示“正在下载 PCAP 包信息”窗口。 在大多数情况下，下载过程非常快，并且不会显示此窗口。

检索到此文件后，将显示一个弹出窗口，其中提供了 PCAP 文件的可读版本。 您可以阅读此窗口上显示的信息，也可以将此信息下载到桌面系统。

过程

1. 对于要调查的事件，选择下列其中一个选项:
   - 选中该事件，然后单击 **PCAP** 图标。
   - 右键单击该事件的 **PCAP** 图标，然后选择**更多选项 > 查看 PCAP 信息**。
   - 双击要调查的事件，然后从事件详细信息工具栏中选择 **PCAP 数据 > 查看 PCAP 信息**。
2. 如果要将此信息下载至桌面系统，请选择下列其中一个选项:
   - 单击**下载 PCAP 文件**以下载原始 PCAP 文件，以便在外部应用程序中使用此文件。
   - 单击**下载 PCAP 文本**以 .TXT 格式下载 PCAP 信息。
3. 选择下列其中一个选项:
   - 如果要打开该文件以便立即查看，请选择**打开方式**选项，然后从列表框中选择应用程序。
   - 如果要保存列表，请选择**保存文件**选项。
4. 单击**确定**。

将 PCAP 文件下载到桌面系统

您可以将 PCAP 文件下载到桌面系统，以进行存储或用于其他应用程序。

开始之前

必须先执行或选择显示了“PCAP 数据”列的搜索，然后才能查看 PCAP 信息。 请参阅**显示 PCAP 数据列**。

过程

1. 对于要调查的事件，选择下列其中一个选项:
   - 选中该事件，然后单击 **PCAP** 图标。
   - 右键单击该事件的 PCAP 图标，然后选择**更多选项 > 下载 PCAP 文件**。
   - 双击要调查的事件，然后从事件详细信息工具栏中选择 **PCAP 数据 > 下载 PCAP 文件**。
2. 选择下列其中一个选项:
   - 如果要打开该文件以便立即查看，请选择**打开方式**选项，然后从列表框中选择应用程序。

- 如果要保存列表，请选择**保存文件**选项。

3. 单击**确定**。

导出事件

您可以采用可扩展标记语言 (XML) 格式或逗号分隔值 (CSV) 格式导出事件。

开始之前

导出数据所需的时间长度取决于指定的参数数目。

过程

1. 单击**日志活动**选项卡。
2. 可选。 如果您是以流方式查看事件，请单击**暂停**图标以暂停流。
3. 从**操作**列表框中，选择下列其中一个选项:
   - **导出为 XML > 可见列** - 选择此选项将仅导出“日志活动”选项卡上显示的列。 建议使用此选项。
   - **导出为 XML > 完全导出（所有列）** - 选择此选项将导出所有事件参数。 完全导出可能需要较长时间才能完成。
   - **导出为 CSV > 可见列** - 选择此选项将仅导出**日志活动**选项卡上显示的列。建议使用此选项。
   - **导出为 CSV > 完全导出（所有列）** - 选择此选项将导出所有事件参数。 完全导出可能需要较长时间才能完成。
4. 如果要在导出进行时继续进行活动，请单击**完成时发送通知**。

结果

导出完成时，您将接收到指示导出完成的通知。 如果您未选择**完成时发送通知**图标，那么将显示“状态”窗口。

第 6 章 网络活动调查

您可以使用**网络活动**选项卡以实时方式监视和调查网络活动（流）或者执行高级搜索

“网络”选项卡概述

通过使用**网络活动**选项卡，您可以实时地监视和调查网络活动（流）或者执行高级搜索。

您必须具有查看**网络活动**选项卡的许可权。

有关许可权和分配角色的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

通过选择**网络活动**选项卡，即可通过可视方式实时监视和调查流数据，或执行高级搜索对显示的流进行过滤。 流是两个主机之间的通信会话。 您可以查看流信息来确定流量的传送方式，以及传送的内容（如果启用了内容捕获选项）。另外，流信息还可以包含协议、自治系统号 (ASN) 值或接口索引 (IFIndex) 值之类的详细信息。

“网络活动”选项卡工具栏

您可以从**网络活动**选项卡工具栏访问多个选项。

您可以从**网络活动**选项卡工具栏访问以下选项:

表 23. “网络活动”选项卡工具栏选项

选项	描述
搜索	单击**搜索**可以对流完成高级搜索。 搜索选项包括: • **新建搜索** - 选择此选项可以创建新的流搜索。 • **编辑搜索** - 选择此选项可以选择并编辑流搜索。 • **管理搜索结果** - 选择此选项可以查看和管理搜索结果。 有关搜索功能的更多信息，请参阅数据搜索。
快速搜索	从这个列表框中，可以运行先前保存的搜索。 仅当已保存指定了**包括在快速搜索中**选项的搜索条件时，**快速搜索**列表框中才会显示选项。
添加过滤器	单击**添加过滤器**可以向当前搜索结果添加过滤器。
保存条件	单击**保存条件**可以保存当前搜索条件。
保存结果	单击**保存结果**可以保存当前搜索结果。只有在完成搜索后，才会显示此选项。在流方式下，此选项处于禁用状态。
取消	单击**取消**可以取消进行中的搜索。 在流方式下，此选项处于禁用状态。

表 23. “网络活动”选项卡工具栏选项 (续)

选项	描述
误报	单击**误报**将打开“误报调整”窗口，以便阻止已确定为误报的流创建攻击。 有关误报的更多信息，请参阅词汇表。 在流方式下，此选项处于禁用状态。请参阅导出流。
规则	仅当您有权查看定制规则时，才会显示**规则**选项。 请选择下列其中一个选项: **规则**，用于查看或创建规则。如果您有权查看规则，那么将显示“规则”向导的摘要页面。 如果您有权维护定制规则，那么可以编辑规则。 **注:** 仅当您具有**网络活动 > 维护定制规则**许可权时，才会显示异常检测规则选项。 要启用异常检测规则选项，您必须保存汇总搜索条件。保存的搜索条件指定了必需参数。 请选择下列其中一个选项 **添加阈值规则**，用于创建阈值规则。 阈值规则对流的流量进行测试，以查找超出了所配置阈值的活动。 阈值可以基于所收集的任何数据。例如，如果您创建了一条阈值规则，指出上午 8 点到下午 5 点之间不得有 220 个以上的客户机登录服务器，那么在第 221 个客户机尝试登录时，此规则将生成警报。 **添加行为规则**，用于创建行为规则。 行为规则对流的流量进行测试，以识别按规律季节性模式发生的行为的量变化。例如，如果邮件服务器在午夜通常每秒与 100 台主机进行通信，然后突然开始每秒与 1,000 台主机进行通信，那么行为规则将生成警报。 **添加异常规则**，用于创建异常规则。 异常规则对流的流量进行测试以识别异常活动，例如新流量或未知流量。 例如，您可以创建一条异常规则，用于将过去 5 分钟的平均流量与过去一小时的平均流量进行比较。如果变化幅度超过 40%，那么此规则将生成响应。 有关更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

表 23. “网络活动”选项卡工具栏选项 (续)

选项	描述
操作	单击**操作**可以完成下列操作: • **全部显示** - 选择此选项可以除去所有对搜索条件应用的过滤器，并显示所有流（未进行过滤）。 • **打印** - 选择此选项可以打印页面上显示的流。 • **导出为 XML** - 选择此选项可以采用 XML 格式导出流。 请参阅导出流。 • **导出为 CSV** - 选择此选项可以采用 CSV 格式导出流。 请参阅导出流。 • **删除** - 选择此选项可以删除搜索结果。 请参阅数据搜索。 • **通知** - 选择此选项可以指定您希望所选搜索完成时通过电子邮件向您发送通知。 仅对于进行中的搜索才会启用此选项。 **注**: 在流方式下，以及在查看不完整的搜索结果时，**打印**、**导出为 XML** 和**导出为 CSV** 选项处于禁用状态。
搜索工具栏	**高级搜索** 从列表框中选择**高级搜索**，然后输入 Ariel Query Language (AQL) 搜索字符串来指定您希望返回的字段。 **快速过滤** 从列表框中选择**快速过滤**以便使用简单字或短语来搜索有效内容。
视图	**网络活动**选项卡上的缺省视图是实时事件流。**视图**列表包含一些选项，也可以用于查看指定时间段内的事件。从**视图**列表中选择指定时间段后，您可以通过更改**开始时间**和**结束时间**字段中的日期和时间值来修改所显示的时间段。

右键单击菜单选项

在**网络活动**选项卡上，可以右键单击流来访问更多流过滤条件。

右键单击菜单选项包括:

表 24. 右键单击菜单选项

选项	描述
过滤	选择此选项可以根据流中的选定参数过滤所选流。
误报	选择此选项可打开“误报调整”窗口，此窗口允许您阻止已确定为误报的流创建攻击。 在流方式下，此选项处于禁用状态。请参阅导出流。
更多选项:	选择此选项可以调查 IP 地址。请参阅调查 IP 地址。 **注**: 在流方式下，不会显示此选项。

表 24. 右键单击菜单选项 (续)

选项	描述
快速过滤	过滤与选定内容匹配或不匹配的项。

状态栏

对流执行流式方法处理时，状态栏将显示每秒接收到的平均结果数。

这是控制台从事件处理器成功接收到的结果数。 如果此数目大于每秒 40 个结果，那么将仅显示 40 个结果。 其余的项将在结果缓冲区中累积。 要查看更多状态信息，请将鼠标指针移动到状态栏上。

未对流执行流式方法处理时，状态栏将显示当前显示的搜索结果数，以及处理搜索结果所需的时间长度。

溢出记录

借助管理许可权，您可以指定要从 QRadar QFlow Collector 发送到事件处理器的最大流数。

如果您具有管理许可权，那么可以指定要从 QRadar QFlow Collector 发送到事件处理器的最大流数。达到配置的流限制之后收集的所有数据将分组到一个流记录中。然后，此流记录将显示在**网络活动**选项卡中并显示源 IP 地址 127.0.0.4 和目标 IP 地址 127.0.0.5。此流记录在**网络活动**选项卡上指定“溢出”。

网络活动监视

缺省情况下，**网络活动**选项卡以流方式显示流，这使您能够实时查看流。

有关流方式的更多信息，请参阅查看流式流。 您可以使用**查看**列表框来指定另一时间范围，以便对流进行过滤。

如果您先前已将某个已保存的搜索配置为缺省搜索，那么您访问**网络活动**选项卡时，会自动显示该搜索的结果。有关保存搜索条件的更多信息，请参阅保存事件和流搜索条件。

查看流式流

流方式使您能够查看进入系统的流数据。 此方式通过显示最近 50 个流为您提供有关当前流活动的实时视图。

关于此任务

如果在启用流方式之前在“网络活动”选项卡或搜索条件中应用了任何过滤器，那么这些过滤器将在流方式下进行维护。 但是，流方式不支持包含已分组流的搜索。 如果对已分组流或已分组搜索条件启用流方式，那么“网络活动”选项卡将显示规范化流。 请参阅『查看规范化流』。

如果要选择一个流以查看详细信息或执行操作，那么必须先暂停流式方法，然后再双击一个事件。 暂停流式方法后，将显示最近 1,000 个流。

过程

1. 单击**网络活动**选项卡。
2. 从“视图”列表框中，选择**实时（流式方法）**。

有关工具栏选项的信息，请参阅表 5-1。 有关流方式下显示的参数的更多信息，请参阅表 5-3。

3. 可选。 暂停或启动流式流。 选择下列其中一个选项:
   - 要选择事件记录，请单击**暂停**图标以暂停流式方法。
   - 要重新启动流方式，请单击**启动**图标。

查看规范化流

数据流将进行收集、规范化然后显示在**网络活动**选项卡中。

关于此任务

规范化涉及准备流数据，以便显示有关选项卡的可读信息。

注: 如果选择了要显示的时间范围，那么将显示一个时间序列图表。 有关使用时间序列图表的更多信息，请参阅时间序列图表概述。

查看规范化流时，**网络活动**选项卡将显示下列参数:

表 25. “网络活动”选项卡的参数

参数	描述
当前过滤器	表顶部显示应用于搜索结果的过滤器的详细信息。 要清除这些过滤器值，请单击**清除过滤器**。 **注**: 仅当您应用过滤器后，才会显示此参数。
视图	从列表框中，可以选择要过滤的时间范围。
当前的统计信息	在“实时（流式方法）”或“上一分钟（自动刷新）”方式以外的方式下，将显示当前统计信息，其中包括: **注**: 单击“当前统计信息”旁边的箭头可以显示或隐藏统计信息。 • **总结果数** - 指定满足搜索条件的结果总数。 • **搜索到的数据文件数** - 指定在指定的时间范围内搜索到的数据文件总数。 • **搜索到的压缩数据文件数** - 指定在指定的时间范围内搜索到的压缩数据文件总数。 • **索引文件计数** - 指定在指定的时间范围内搜索到的索引文件总数。 • **持续时间** - 指定搜索的持续时间。 **注**: 当前统计信息对于故障诊断而言非常有用。 联系客户支持以便对流进行故障诊断时，可能会要求您提供当前统计信息。

表 25. “网络活动”选项卡的参数 (续)

参数	描述
图表	显示可配置图表，这些图表表示与时间间隔和分组选项相匹配的记录。 如果不希望显示图表，请单击**隐藏图表**。 仅当您选择上次时间间隔（自动刷新）或更广的时间范围，并且选择要显示的分组选项后，才会显示图表。 有关配置图表的更多信息，请参阅配置图表。 **注**: 如果您使用 Mozilla Firefox 作为浏览器，并且安装了广告拦截器浏览器扩展，那么图表无法显示。 要显示图表，必须除去广告拦截器浏览器扩展。 有关更多信息，请参阅浏览器文档。
攻击图标	单击**攻击**图标可以查看与此流相关联的攻击的详细信息。
流类型	指定流类型。 流类型以传入活动相对传出活动的比率测量。 流类型包括: • **标准流** - 双向流量 • **A 类** - 一对多（单向），例如，执行网络扫描的单个主机。 • **B 类** - 多对一（单向），例如，分布式 DoS (DDoS) 攻击。 • **C 类** - 一对一（单向），例如，主机到主机端口扫描。
第一个包的时间	指定接收流的日期和时间。
存储时间	指定将此流存储到 QRadar 数据库的时间。
源 IP	指定此流的源 IP 地址。
源端口	指定此流的源端口。
目标 IP	指定此流的目标 IP 地址。
目标端口	指定此流的目标端口。
源字节数	指定从源主机发送的字节数。
目标字节数	指定从目标主机发送的字节数。
总字节数	指定与此流相关联的总字节数。
源数据包数	指定从源主机发送的总包数。
目标数据包数	指定从目标主机发送的总包数。
数据包总数	指定与此流相关联的总包数。
协议	指定与此流相关联的协议。
应用程序	指定检测到的流应用程序。 有关应用程序检测的更多信息，请参阅 *IBM Security QRadar Application Configuration Guide*。

表 25. “网络活动”选项卡的参数 (续)

参数	描述
ICMP 类型/代码	指定因特网控制报文协议 (ICMP) 类型和代码（如果适用）。 如果流具有格式已知的 ICMP 类型和代码信息，那么此字段显示为 Type <A>. Code <B>, 其中 <A> 和 <B> 是类型和代码的数字值。
源标志	指定源包中检测到的传输控制协议 (TCP) 标志（如果适用）。
目标标志	指定目标包中检测到的 TCP 标志（如果适用）。
源 QoS	指定此流的服务质量 (QoS) 服务级别。 QoS 使网络能够为流提供各种服务级别。 QoS 提供了下列基本服务级别: • **最佳服务** - 此服务级别不保证交付。 交付流被视作最佳服务。 • **差别服务** - 对某些流授予了高于其他流的优先级。 此优先级通过流量分类授予。 • **保证服务** - 此服务级别保证为某些流预留网络资源。
目标 QoS	指定目标流的 QoS 服务级别。
流源	指定检测到流的系统。
流接口	指定接收流的接口。
源 IFIndex	指定源接口索引 (IFIndex) 号。
目标 IFIndex	指定目标 IFIndex 编号。
源 ASN	指定源自治系统号 (ASN) 值。
目标 ASN	指定目标 ASN 值。

过程

1. 单击**网络活动**选项卡。
2. 从**显示**列表框中，选择**缺省值（规范化）**。
3. 从**视图**列表框中，选择要显示的时间范围。
4. 单击**暂停**图标以暂停流式方法。
5. 双击要查看其详细信息的流。 请参阅流详细信息。

查看已分组的流

通过使用**网络活动**选项卡，您可以查看按各个选项进行了分组的流。 您可以从**显示**列表框中选择要作为流分组依据的参数。

关于此任务

流方式不支持已分组的流，因此，在流方式下**显示**列表框不会显示。 如果您使用不分组搜索条件进入了流方式，那么将显示此选项。

显示列表框提供了下列选项:

表 26. 分组流选项

组选项	描述
源或目标 IP	显示按与流相关联的 IP 地址分组的流的汇总列表。
源 IP	显示按流的源 IP 地址分组的流的汇总列表。
目标 IP	显示按流的目标 IP 地址分组的流的汇总列表。
源端口	显示按流的源端口分组的流的汇总列表。
目标端口	显示按流的目标端口分组的流的汇总列表。
源网络	显示按流的源网络分组的流的汇总列表。
目标网络	显示按流的目标网络分组的流的汇总列表。
应用程序	显示按发起流的应用程序分组的流的汇总列表。
地理投影	显示按地理位置分组的流的汇总列表。
协议	显示按与流相关联的协议分组的流的汇总列表。
流偏置	显示按流方向分组的流的汇总列表。
ICMP 类型	显示按流的 ICMP 类型分组的流的汇总列表。

从**显示**列表框中选择一个选项后，数据的列布局将取决于所选组选项。流表中的每行都表示一个流组。 **网络活动**选项卡提供了各个流组的以下信息。

表 27. 分组流参数

标题	描述
分组依据	指定作为搜索分组依据的参数。
当前过滤器	表顶部显示应用于搜索结果的过滤器的详细信息。 要清除这些过滤器值，请单击**清除过滤器**。
视图	从列表框中，选择要过滤的时间范围。
当前统计信息	在“实时（流式方法）”或“上一分钟（自动刷新）”方式以外的方式下，将显示当前统计信息，其中包括: **注**: 单击**当前统计信息**旁边的箭头可以显示或隐藏统计信息。 • **总结果数** - 指定满足搜索条件的结果总数。 • **搜索到的数据文件数** - 指定在指定的时间范围内搜索到的数据文件总数。 • **搜索到的压缩数据文件数** - 指定在指定的时间范围内搜索到的压缩数据文件总数。 • **索引文件计数** - 指定在指定的时间范围内搜索到的索引文件总数。 • **持续时间** - 指定搜索的持续时间。 **注**: 当前统计信息对于故障诊断而言非常有用。 联系客户支持以便对流进行故障诊断时，可能会要求您提供当前统计信息。

表 27. 分组流参数 (续)

标题	描述
图表	显示可配置图表，这些图表表示与时间间隔和分组选项相匹配的记录。如果不希望显示图形，请单击**隐藏图表**。 仅当您选择上次时间间隔（自动刷新）或更广的时间范围，并且选择要显示的分组选项后，才会显示图表。 有关配置图表的更多信息，请参阅配置图表。 **注**: 如果您使用 Mozilla Firefox 作为浏览器，并且安装了广告拦截器浏览器扩展，那么图表无法显示。要显示图表，必须除去广告拦截器浏览器扩展。有关更多信息，请参阅浏览器文档。
源 IP（唯一计数）	指定此流的源 IP 地址。
目标 IP（唯一计数）	指定此流的目标 IP 地址。 如果存在多个与此流相关联的目标 IP 地址，那么此字段将显示“多个”一词以及 IP 地址数。
源端口（唯一计数）	显示此流的源端口。
目标端口（唯一计数）	指定此流的目标端口。如果存在多个与此流相关联的目标端口，那么此字段将显示“多个”一词以及端口数。
源网络（唯一计数）	指定此流的源网络。 如果存在多个与此流相关联的源网络，那么此字段将显示“多个”一词以及网络数。
目标网络（唯一计数）	指定此流的目标网络。如果存在多个与此流相关联的目标网络，那么此字段将显示“多个”一词以及网络数。
应用程序（唯一计数）	指定检测到的流应用程序。如果存在多个与此流相关联的应用程序，那么此字段将显示“多个”一词以及应用程序数。
源字节数（总和）	指定来自源的字节数。
目标字节数（总和）	指定来自目标的字节数。
总字节数（总和）	指定与此流相关联的总字节数。
源包数（总和）	指定来自源的包数。
源包数（总和）	指定来自源的包数。
源包数（总和）	指定来自源的包数。
目标包数（总和）	指定来自目标的包数。
数据包总数（总和）	指定与此流相关联的总包数。
计数	指定发送或接收的包数。

过程

1. 单击**网络活动**选项卡。
2. 从**视图**列表框中，选择要显示的时间范围。

3. 从**显示**列表框中，选择要作为流分组依据的参数。 请参阅表 2。 列出了流组。 有关流组详细信息的更多信息， 请参阅表 1。
4. 要查看某个组的“流列表”页面，请双击要调查的流组。 “流列表”页面未保留您可能已在**网络活动**选项卡中定义的图表配置。 有关流列表参数的更多信息，请参阅表 2。
5. 要查看某个流的详细信息，请双击要调查的流。 有关流详细信息页面的更多信息，请参阅表 1。

流详细信息

您可以通过各种方式（包括流方式或流组方式）查看流列表。 无论您选择以何种方式查看流，都可以查找并查看单个流的详细信息。

流详细信息页面提供了以下信息:

表 28. 流详细信息

参数	描述
流信息	
协议	指定与此流关联的协议。 有关协议的更多信息，请参阅 *IBM Security QRadar Application Configuration Guide*。
应用程序	指定检测到的流应用程序。有关应用程序检测的更多信息，请参阅 *IBM Security QRadar Application Configuration Guide*。
规模	指定此流的规模。 有关规模的更多信息，请参阅词汇表。
相关性	指定此流的相关性。 有关相关性的更多信息，请参阅词汇表。
严重性	指定此流的严重性。 有关严重性的更多信息，请参阅词汇表。
可信性	指定此流的可信性。 有关可信性的更多信息，请参阅词汇表。
第一个包的时间	指定流源所报告的流开始时间。 有关流源的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
最后一个包的时间	指定流源所报告的流结束时间。
存储时间	指定将此流存储到 QRadar 数据库的时间。
事件名称	指定此流的规范化名称。
低级别类别	指定此流的低级别类别。 有关类别的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
事件描述	指定此流的描述（如果有）。
源及目标信息	
源 IP	指定此流的源 IP 地址。
目标 IP	指定此流的目标 IP 地址。

表 28. 流详细信息 (续)

参数	描述
源资产名称	指定此流的源资产名称。有关资产的更多信息，请参阅资产管理。
目标资产名称	指定此流的目标资产名称。 有关资产的更多信息，请参阅资产管理。
IPv6 源	指定此流的源 IPv6 地址。
IPv6 目标	指定此流的目标 IPv6 地址。
源端口	指定此流的源端口。
目标端口	指定此流的目标端口。
源 QoS	指定源流的 QoS 服务级别。
目标 QoS	指定目标流的 QoS 服务级别。
源 ASN	指定源 ASN 编号。 **注**: 如果此流包含来自多个流源的重复记录，那么将列出对应的源 ASN 编号。
目标 ASN	指定目标 ASN 编号。 **注**: 如果此流包含来自多个流源的重复记录，那么将列出对应的目标 ASN 编号。
源 IFIndex	指定源 IFIndex 编号。 **注**: 如果此流包含来自多个流源的重复记录，那么将列出对应的源 IFIndex 编号。
目标 IFIndex	指定目标 IFIndex 编号。 **注**: 如果此流包含来自多个流源的重复记录，那么将列出对应的源 IFIndex 编号。
源有效内容	指定源有效内容的包和字节计数。
目标有效内容	指定目标有效内容的包和字节计数。
有效内容信息	
源有效内容	指定流中的源有效内容。此字段提供了 3 种格式，用于查看有效内容: • 通用转换格式 (UTF) - 请单击 UTF。 • 十六进制 - 请单击 HEX。 • Base64 - 请单击 Base64。 **注**: 如果流源是 Netflow V9 或 IPFIX，那么这些源中未解析的字段可能会显示在**源有效内容**字段中。 未解析字段的格式为 <name>=<value>。例如，`MN_TTL=x`
目标有效内容	指定流中的目标有效内容。 此字段提供了 3 种格式，用于查看有效内容: • 通用转换格式 (UTF) - 请单击 **UTF**。 • 十六进制 - 请单击 **HEX**。 • Base64 - 请单击 **Base64**。
其他信息	

表 28. 流详细信息 (续)

参数	描述
流类型	指定流类型。流类型以传入活动相对传出活动的比率测量。流类型包括: • 标准 - 双向流量 • A 类 - 一对多（单向） • B 类 - 多对一（单向） • C 类 - 一对一（单向）
流方向	指定流方向。 流方向包括: • L2L - 从本地网络到另一本地网络的内部流量。 • L2R - 从本地网络到远程网络的内部流量。 • R2L - 从远程网络到本地网络的内部流量。 • R2R - 从远程网络到另一远程网络的内部流量。
定制规则	指定与此流匹配的定制规则。 有关规则的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
部分匹配的定制规则	指定与此流部分匹配的定制规则。
流源/接口	指定检测到流的系统的流源名称。 **注**: 如果此流包含来自多个流源的重复记录，那么将列出对应的流源。
注释	指定此流的注释或备注。注释是规则可以对流自动添加的文本描述，作为规则响应的组成部分。

“流详细信息”工具栏

“流详细信息”工具栏提供了多项功能。

“流详细信息”工具栏提供了下列功能

表 29. “流详细信息”工具栏的描述

功能	描述
返回到结果	单击**返回到结果**可以返回到流列表。
抽取属性	单击**抽取属性**可以根据选择的流创建定制流属性。 有关更多信息，请参阅『事件和流的定制属性』。
误报	单击**误报**将打开“误报调整”窗口，此窗口允许您阻止已确定为误报的流创建攻击。 在流方式下，此选项处于禁用状态。请参阅导出流。
上一个	单击**上一个**可以查看流列表中的上一个流。
下一个	单击**下一个**可以查看流列表中的下一个流。
打印	单击**打印**可以打印流详细信息。

表 29. “流详细信息”工具栏的描述 (续)

功能	描述
攻击	如果**攻击**可用，单击即可查看“攻击摘要”页面。

调整误报

使用“误报调整”功能可以阻止误报流创建攻击。 您可以从流列表或流详细信息页面调整误报流。

关于此任务

注: 您可以从摘要或详细信息页面调整误报流。

您必须具有创建定制规则的相应许可权才能调整误报。 有关误报的更多信息，请参阅词汇表。

过程

1. 单击**网络活动**选项卡。
2. 可选。 如果您是以流方式查看流，请单击**暂停**图标以暂停流。
3. 选择要调整的流。
4. 单击**误报**。
5. 在“误报”窗口上的“事件/流属性”窗格中，选择下列其中一个选项:
   - 具有特定 QID <Event> 的事件/流
   - 任何具有低级别类别 <Event> 的事件/流
   - 任何具有高级别类别 <Event> 的事件/流
6. 在“流量方向”窗格中，选择下列其中一个选项:
   - <源 IP 地址> 到 <目标 IP 地址>
   - <源 IP 地址> 到任何目标
   - 任何源到 <目标 IP 地址>
   - 任何源到任何目标
7. 单击**调整**。

导出流

您可以采用可扩展标记语言 (XML) 格式或逗号分隔值 (CSV) 格式导出流。 导出数据所需的时间长度取决于指定的参数数目。

过程

1. 单击**网络活动**选项卡。
2. 可选。 如果您是以流方式查看流，请单击**暂停**图标以暂停流。
3. 从**操作**列表框中，选择下列其中一个选项:
   - **导出为 XML > 可见列** - 选择此选项将仅导出“日志活动”选项卡上显示的列。 建议使用此选项。

- **导出为 XML > 完全导出（所有列）** - 选择此选项将导出所有流参数。 完全导出可能需要较长时间才能完成。
- **导出为 CSV > 可见列** - 选择此选项将仅导出“日志活动”选项卡上显示的列。 建议使用此选项。
- **导出为 CSV > 完全导出（所有列）** - 选择此选项将导出所有流参数。 完全导出可能需要较长时间才能完成。

4. 如果要继续进行活动，请单击**完成时发送通知**。

结果

导出完成时，您将接收到指示导出完成的通知。 如果您未选择**完成时发送通知**图标，那么将显示“状态”窗口。

第 7 章 资产管理

收集和查看资产数据有助于识别威胁和漏洞。 通过准确的资产数据库，可以更轻松地将系统中触发的攻击与网络中的物理资产和虚拟资产相关联。

限制: 只有在安装了 QRadar Vulnerability Manager 时，QRadar Log Manager 才会跟踪资产数据。有关 IBM Security QRadar SIEM 与 IBM Security QRadar Log Manager 之间的差异的更多信息，请参阅 第 5 页的『安全情报产品中的功能』。

资产数据

资产是跨网络基础结构发送或接收数据的任意网络端点。例如，笔记本、服务器、虚拟机和手持设备全都是资产。 资产数据库中的每个资产分配有唯一标识，以便可以将其与其他资产记录区分。

检测设备还有助于构建有关资产的历史信息的数据集。 随着资产的更改跟踪其信息有助于监视整个网络的资产使用情况。

资产概要信息

*资产概要文件*是 IBM Security QRadar SIEM 长期收集的有关特定资产的所有信息的集合。 概要文件包括有关资产上运行的服务的信息以及已知的任何身份信息。

QRadar SIEM 根据身份事件和双向流数据或在二者已配置的情况下根据漏洞评估扫描自动创建资产概要文件。 数据通过名为*资产协调*的过程进行关联，并且在新信息进入到 QRadar 中时会更新概要文件。资产名称按以下优先顺序派生自资产更新中的信息:

- 指定的名称
- NETBios 主机名
- DNS 主机名
- IP 地址

收集资产数据

资产概要文件将根据从事件或流数据被动获得的身份信息动态构建，或者根据在脆弱性扫描期间 QRadar 主动查找到的数据动态构建。您也可以手动导入资产数据或编辑资产概要文件。

资产数据的源

资产数据接收自 IBM Security QRadar 部署中的若干不同的源。

资产数据会递增写入到资产数据库中（通常一次两个或三个数据段）。 除网络漏洞扫描程序进行的更新以外，每个资产更新一次仅包含有关一个资产的信息。

资产数据通常来自以下资产数据源之一:

事件数 事件有效内容（如 DHCP 或认证服务器创建的有效内容）通常包含用户登录、

IP 地址、主机名、MAC 地址和其他资产信息。 此数据会立即提供给资产数据库，以帮助确定资产更新适用于的资产。

事件是资产增长偏差的主要原因。

流

流有效内容包含按定期、可配置时间间隔收集的通信信息，如 IP 地址、端口和协议。在每个时间间隔结束时，会将数据提供给资产数据库（一次一个 IP 地址）。

由于流中的资产数据根据单一标识（即 IP 地址）与资产配对，因此流数据绝不会导致资产增长偏差。

漏洞扫描程序

QRadar 与 IBM 和第三方漏洞扫描程序集成，这些漏洞扫描程序可以提供资产数据，如操作系统、已安装的软件和补丁信息。 数据的类型根据扫描程序而异，并且可以因扫描而异。 随着新的资产、端口信息和漏洞的发现，会根据扫描中定义的 CIDR 范围将数据引入到资产概要文件中。

扫描程序可能会造成资产增长偏差，但是该情况比较少见。

用户界面

具有“资产”角色的用户可以将资产信息直接导入到或提供给资产数据库。 由用户直接提供的资产更新用于特定资产，因此会绕过资产协调阶段。

用户提供的资产更新不会造成资产增长偏差。

域感知资产数据

使用域信息来配置资产数据源时，来自该数据源的所有资产数据都自动通过同一个域进行标记。 由于资产模型中的数据可感知域，因此域信息会应用于所有 QRadar 组件，包括身份、攻击、资产概要文件和服务器发现。

查看资产概要文件时，某些字段可能为空白。 当系统在资产更新中未接收此信息，或者信息超过资产保留期时，空白字段存在。 缺省保留期为 120 天。 显示为 0.0.0.0 的 IP 地址指示资产不包含 IP 地址信息。

传入资产数据的工作流程

此工作流程描述 QRadar 在事件有效内容中如何使用身份信息来确定要创建新资产还是更新现有资产。

1. QRadar 接收事件。 资产概要分析程序检查事件有效内容以获取身份信息。
2. 如果身份信息包含已经与资产数据库中的资产关联的 MAC 地址、NetBIOS 主机名或 DNS 主机名，那么会使用任何新信息更新该资产。
3. 如果仅有的可用身份信息是 IP 地址，那么系统会协调对具有同一 IP 地址的现有资产的更新。
4. 如果资产更新包含与现有资产匹配的 IP 地址，但也包含更多与现有资产不匹配的身份信息，那么在更新现有资产之前，系统会使用其他信息来排除误报匹配。
5. 如果身份信息与数据库中的现有资产不匹配，那么会根据事件有效内容中的信息创建新资产。

资产数据更新

IBM Security QRadar 在事件有效内容中使用身份信息来确定要创建新资产还是更新现有资产。

每个资产更新都必须包含有关单个资产的可信信息。 当 QRadar 接收资产更新时，系统会确定更新应用于的资产。

*资产协调*是确定资产更新与资产数据库中的相关资产之间关系的过程。 资产协调在 QRadar 接收更新后但在信息写入到资产数据库中之前发生。

身份信息

每个资产都必须包含至少一段身份数据。 包含一段或多段该相同身份数据的后续更新会与拥有该数据的资产进行协调。 将会仔细处理基于 IP 地址的更新，以避免误报资产匹配。 当一个物理资产分配有先前由系统中的另一个资产所有的 IP 地址的所有权时，会发生误报资产匹配。

当提供了多段身份数据时，资产概要分析程序按以下顺序划分信息优先级:

- MAC 地址（最确定）
- NetBIOS 主机名
- DNS 主机名
- IP 地址（最不确定）

MAC 地址、NetBIOS 主机名和 DNS 主机名必须唯一，因此被视为最终身份数据。 仅按 IP 地址与现有资产匹配的入局更新的处理方式不同于与更确定的身份数据匹配的更新。

相关概念:

『资产协调排除规则』

通过进入 IBM Security QRadar 的每个资产更新，资产协调排除规则将测试应用于资产更新中的 MAC 地址、NetBIOS 主机名、DNS 主机名和 IP 地址。

资产协调排除规则

通过进入 IBM Security QRadar 的每个资产更新，资产协调排除规则将测试应用于资产更新中的 MAC 地址、NetBIOS 主机名、DNS 主机名和 IP 地址。

缺省情况下，会对每个资产数据段进行为期两小时的跟踪。 如果资产更新中的任何一段身份数据在 2 小时内展现两次或以上的可疑行为，那么会将该数据段添加到资产黑名单。 针对所测试的每种身份资产数据有一个单独的黑名单。

在域感知环境中，资产协调排除规则为每个域单独跟踪资产数据的行为。

资产协调排除规则测试以下场景:

表 30. 规则测试和响应

场景	规则响应
MAC 地址在 2 小时或更短时间内与三个或更多不同 IP 地址关联	将 MAC 地址添加到资产协调域 MAC 黑名单

表 30. 规则测试和响应 (续)

场景	规则响应
DNS 主机名在 2 小时或更短时间内与三个或更多不同 IP 地址关联	将 DNS 主机名添加到资产协调域 DNS 黑名单
NetBIOS 主机名在 2 小时或更短时间内与三个或更多不同 IP 地址关联	将 NetBIOS 主机名添加到资产协调域 NetBIOS 黑名单
IPv4 地址在 2 小时或更短时间内与三个或更多不同 MAC 地址关联	将 IP 地址添加到资产协调域 IPv4 黑名单
NetBIOS 主机名在 2 小时或更短时间内与三个或更多不同 MAC 地址关联	将 NetBIOS 主机名添加到资产协调域 NetBIOS 黑名单
DNS 主机名在 2 小时或更短时间内与三个或更多不同 MAC 地址关联	将 DNS 主机名添加到资产协调域 DNS 黑名单
IPv4 地址在 2 小时或更短时间内与三个或更多不同 DNS 主机名关联	将 IP 地址添加到资产协调域 IPv4 黑名单
NetBIOS 主机名在 2 小时或更短时间内与三个或更多不同 DNS 主机名关联	将 NetBIOS 主机名添加到资产协调域 NetBIOS 黑名单
MAC 地址在 2 小时或更短时间内与三个或更多不同 DNS 主机名关联	将 MAC 地址添加到资产协调域 MAC 黑名单
地址在 2 小时或更短时间内与三个或更多不同 NetBIOS 主机名关联	将 IP 地址添加到资产协调域 IPv4 黑名单
DNS 主机名在 2 小时或更短时间内与三个或更多不同 NetBIOS 主机名关联	将 DNS 主机名添加到资产协调域 DNS 黑名单
MAC 地址在 2 小时或更短时间内与三个或更多不同 NetBIOS 主机名关联	将 MAC 地址添加到资产协调域 MAC 黑名单

您可以在**攻击**选项卡上查看这些规则，方法是单击**规则**，然后在下拉列表中选择**资产协调排除**组。

相关概念:

『示例: 调整为从黑名单中排除 IP 地址的资产排除规则』
您可以通过调整资产排除规则使 IP 地址避免列入黑名单。

示例: 调整为从黑名单中排除 IP 地址的资产排除规则

您可以通过调整资产排除规则使 IP 地址避免列入黑名单。

作为网络安全性管理员，您管理的是包含公共 wifi 网段的公司网络，其中 IP 地址租赁通常时间短且频繁。 此网段上的资产趋于瞬态，主要是频繁登录和注销公共 wifi 的笔记本和手持设备。 通常，一个 IP 地址在短期内由不同设备多次使用。

在其余部署中，您具有一个仔细管理的网络，其中仅包含已盘点的知名公司设备。 IP 地址在此部分的网络中租赁时间更长，并且 IP 地址仅通过认证进行访问。 在此网段上，您希望在有任何资产增长偏差时立即获知情况，并且保留资产协调排除规则的缺省设置。

将 IP 地址列入黑名单

在此环境中，缺省资产协调排除规则会无意间将整个网络短期列入黑名单。

您的安全团队发现 wifi 网段生成的资产相关通知惹人讨厌。 您希望防止 wifi 触发任何其他偏差资产增长通知。

调整资产协调规则以忽略某些资产更新

复审上次系统通知中的**由日志源导致的资产偏差**报告。 确定列入黑名单的数据是来自 您的 wifi 上的 DHCP 服务器。

与**资产排除: 按 MAC 地址排除 IP** 规则对应的行的**事件计数**列、**流计数**列和**攻击**列中的值指示是您的 wifi DHCP 服务器在触发此规则。

向现有资产协调排除规则中添加测试可阻止规则将 wifi 数据添加到黑名单。

```
Apply AssetExclusion:Exclude IP by MAC address on events which are detected by
the Local system and NOT when the event(s) were detected by one or more of
MicrosoftDHCP @ microsoft.dhcp.test.com
and NOT when any of Domain is the key and any of Identity IP is the value in
any of Asset Reconciliation Domain IPv4 Whitelist
- IP Asset Reconciliation Domain IPv4 Blacklist - IP
and when at least 3 events are seen with the same Identity IP and
different Identity MAC in 2 hours.
```

已更新的规则仅测试来自您的 wifi DHCP 服务器上没有的日志源的事件。 为防止 wifi DHCP 事件经历更高昂的引用集和行为分析测试，您还将此测试移至测试堆栈的顶部

资产合并

*资产合并*是一个资产的信息与另一个资产的信息进行组合的过程（前提是两个资产实际是同一物理资产）。

当资产更新包含与两个不同资产概要文件匹配的身份数据时，会发生资产合并。 例如，如果单个更新包含与一个资产概要文件匹配的 NetBIOS 主机名和与另一个资产概要文件匹配的 MAC 地址，那么该更新可能会触发资产合并。

某些系统会导致大量资产合并，因为它们具有会在无意间将两个不同物理资产的身份信息组合成单个资产更新的资产数据源。 这些系统的一些示例包括以下环境:

- 充当事件代理的中央系统日志服务器
- 虚拟机
- 自动化安装环境
- 非唯一主机名，与 iPad 和 iPhone 之类的资产通用。
- 具有共享 MAC 地址的虚拟专用网
- 日志源扩展，其中身份字段为 `OverrideAndAlwaysSend=true`

具有多个 IP 地址、MAC 地址或主机名的资产在资产增长中显示偏差，并且会触发系统通知。

相关概念:

第 102 页的『识别资产增长偏差』

有时，资产数据源会产生必须进行手动补救后 IBM Security QRadar 才能正确处理的更新。根据异常资产增长的原因，您可以修正引起问题的资产数据源，或者阻止来自该数据源的资产更新。

识别资产增长偏差

有时，资产数据源会产生必须进行手动补救后 IBM Security QRadar 才能正确处理的更新。根据异常资产增长的原因，您可以修正引起问题的资产数据源，或者阻止来自该数据源的资产更新。

当单个设备的资产更新数超过特定类型身份信息的保留时间阈值所设置的限制时，即发生*资产增长偏差*。正确处理资产增长偏差对于维护准确的资产模型而言非常关键。

每项资产增长偏差的根源是一个资产数据源，其数据不可信，不应用来更新资产模型。识别潜在的资产增长偏差之后，您必须检查信息源，以确定能否合理解释该资产为何积累大量身份数据。资产增长偏差的原因随环境不同而异。

资产概要文件中异常数据增长的 DHCP 服务器示例

假如在动态主机配置协议 (DHCP) 网络中有一个虚拟专用网 (VPN) 服务器。 该 VPN 服务器配置为通过代表客户机将 DHCP 请求以代理形式发送到该网络的 DHCP 服务器来将 IP 地址分配给入局 VPN 客户机。

从 DHCP 服务器的角度而言，同一 MAC 地址重复请求许多 IP 地址分配。 在网络操作的上下文中，VPN 服务器将 IP 地址委派给客户机，但是 DHCP 服务器在请求是由一个资产代表另一个资产发出时无法进行区分。

DHCP 服务器日志（配置为 QRadar 日志源）会生成 DHCP 应答 (DHCP ACK) 事件，该事件将 VPN 服务器的 MAC 地址与分配给 VPN 客户机的 IP 地址关联。 当发生资产协调时，系统按 MAC 地址协调此事件，从而导致单个现有资产针对所解析的每个 DHCP ACK 事件按一个 IP 地址进行增长。

最终，一个资产概要文件会包含分配给 VPN 服务器的每个 IP 地址。 此资产增长偏差由包含有关多个资产的信息的资产更新所导致。

阈值设置

当数据库中的资产达到特定的属性数量（如多个 IP 地址或 MAC 地址）时，那么 QRadar 会阻止该资产接收更多更新。

资产概要分析程序阈值设置指定阻止资产更新所处的条件。 资产的更新数通常最多为阈值。 当系统收集足够的数据而超过阈值时，资产会显示资产增长偏差。 这会阻止资产的未来更新，直至修正增长偏差为止。

指示资产增长偏差的系统通知

IBM Security QRadar 生成系统通知来帮助您标识和管理环境中的资产增长偏差。

以下系统消息指示 QRadar 已识别潜在资产增长偏差:

- `The system detected asset profiles that exceed the normal size threshold`
- `The asset blacklist rules have added new asset data to the asset blacklists`

系统通知消息包含指向用于帮助识别具有增长偏差的资产的报告的链接。

频繁更改的资产数据

资产增长可能是由大量合法更改的资产数据所致，例如下列情况下的更改:

- 一台移动设备频繁地从一间办公室转到另一间办公室，并且每次登录时都被赋予新的 IP 地址。
- 连接到采用较短 IP 地址租约的公用 Wi-Fi（例如大学校园中的公用 Wi-Fi）的设备在一个学期内可能会收集到大量资产数据。

示例: 日志源扩展的配置错误如何导致资产增长偏差

配置不正确的定制日志源扩展会导致资产增长偏差。

通过解析位于中央日志服务器上的事件有效内容中的用户名，可以配置定制日志源扩展来向 QRadar 提供资产更新。 将日志源扩展配置为覆盖事件主机名属性，以便定制日志源生成的资产更新始终指定中央日志服务器的 DNS 主机名。

日志源会生成许多全都具有同一主机名的资产更新，而不是由 QRadar 接收具有用户已登录到的资产的主机名的更新。

在此情况下，资产增长偏差由一个包含许多 IP 地址和用户名的资产概要文件导致。

对超过正常大小阈值的资产概要文件进行故障诊断

当单个资产下的数据累计超过所配置的身份数据阈值限制时，IBM Security QRadar 会生成以下系统通知。

```
The system detected asset profiles that exceed the normal size threshold
```

说明

通知的有效内容显示一个列表，其中包含五个偏差最频繁的资产以及系统将每个资产标记为增长偏差的原因。 如以下示例中所示，有效内容还显示资产尝试增长超过资产大小阈值的次数。

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

当资产数据超过所配置的阈值时，QRadar 会阻止资产将来进行更新。 此干预防止系统接收更多损坏的数据，并且降低在系统尝试针对异常大的资产概要文件来协调入局更新时可能出现的性能影响。

必需用户操作

使用通知有效内容中的信息来识别造成资产增长偏差的资产并确定导致异常增长的原因。 通知提供指向在过去 24 小时遭遇资产增长偏差的所有资产的报告的链接。

解决环境中的资产增长偏差后，可以再次运行报告。

1. 单击**日志活动**选项卡，然后单击**搜索 > 新建搜索**。
2. 选择保存的搜索**偏差资产增长: 资产报告**。

3. 使用报告识别并修复在偏差期间创建的不准确资产数据。

如果资产数据有效，那么 QRadar 管理员可以在 QRadar **管理** 选项卡上的**资产概要分析程序配置**中增大 IP 地址、MAC 地址、NetBIOS 主机名和 DNS 主机名的阈值限制。

向资产黑名单中添加了新资产数据

当某个资产数据段展现与造成资产增长偏差一致的行为时，IBM Security QRadar 会生成以下系统通知。

`The asset blacklist rules have added new asset data to the asset blacklists`

说明

资产排除规则监视资产数据的一致性和完整性。 规则长期跟踪特定资产数据段，以确保在合理时间内通过与同一数据子集一致的方式对其进行观察。

例如，如果资产更新包含 MAC 地址和 DNS 主机名，那么 MAC 地址在某个持续时间段与该 DNS 主机名关联。 当资产更新中包含 DNS 主机名时，包含该 MAC 地址的后续资产更新也包含同一 DNS 主机名。 如果 MAC 地址突然短期与其他 DNS 主机名关联，那么会监视更改。如果 MAC 地址短期内再次更改，那么会将 MAC 地址标记为可造成资产增长偏差或异常情况。

必需用户操作

使用通知有效内容中的信息来识别用于监视资产数据的规则。 单击通知中的**资产偏差（按日志源划分）**链接可查看过去 24 小时发生的资产偏差。

如果资产数据有效，那么 QRadar 管理员可以配置 QRadar 来解决问题。

- 如果黑名单的填充过于激烈，那么可以调整用于填充这些黑名单的资产协调排除规则。
- 如果要将数据添加到资产数据库中，那么可以从黑名单中除去资产数据并将其添加到对应的资产白名单。 将资产数据添加到白名单可防止其在黑名单上意外重新出现。

资产黑名单和白名单

IBM Security QRadar 使用一组资产协调规则来确定资产数据是否可信。资产数据存疑时，QRadar 使用资产黑名单和白名单来确定是否使用资产数据来更新资产概要文件。

*资产黑名单*是 IBM Security QRadar 认为不可信的数据集合。资产黑名单中的数据可能会造成资产增长偏差，因此 QRadar 防止将数据添加到资产数据库中。

*资产白名单*是资产数据的集合，它覆盖有关要将哪些数据添加至资产黑名单的资产协调引擎逻辑。当系统识别黑名单匹配项时，它将检查白名单，以确定该值是否存在。如果该资产更新与白名单中的数据匹配，那么将协调该更改并更新该资产。列入白名单的资产数据针对所有域进行全局应用。

QRadar 管理员可以修改资产黑名单和白名单数据，以防止未来的资产增长偏差。

资产黑名单

*资产黑名单*是 IBM Security QRadar 根据资产年协调排除规则认为不可信的数据的集合。资产黑名单中的数据可能会造成资产增长偏差，因此 QRadar 防止将数据添加到资产数据库中。

QRadar 中的每个资产更新都会与资产黑名单相比较。 列入黑名单的资产数据针对所有域进行全局应用。 如果资产更新包含在黑名单上找到的身份信息（MAC 地址、NetBIOS 主机名、DNS 主机名或 IP 地址），那么会废弃入局更新且不更新资产数据库。

下表显示每种身份资产数据的引用集合名称和类型。

表 31. 资产黑名单数据的引用集合名称

身份数据的类型	引用集合名称	引用集合类型
IP 地址 (v4)	资产协调 IPv4 黑名单	引用集 [集类型: IP]
DNS 主机名	资产协调 DNS 黑名单	引用集 [集类型: ALNIC*]
NetBIOS 主机名	资产协调 NetBIOS 黑名单	引用集 [集类型: ALNIC*]
MAC 地址	资产协调 MAC 黑名单	引用集 [集类型: ALNIC*]
* ALNIC 是可以同时适应主机名值和 MAC 地址值的字母数字类型。		

QRadar 管理员可以修改黑名单条目，以确保正确处理资产数据。

资产白名单

您可使用资产白名单来确保 IBM Security QRadar 资产数据不会意外地重新出现在资产黑名单中。

*资产白名单*是资产数据的集合，它覆盖有关要将哪些数据添加至资产黑名单的资产协调引擎逻辑。当系统识别黑名单匹配项时，它将检查白名单，以确定该值是否存在。如果该资产更新与白名单中的数据匹配，那么将协调该更改并更新该资产。列入白名单的资产数据针对所有域进行全局应用。

QRadar 管理员可以修改白名单条目，以确保正确处理资产数据。

白名单用例示例

存在继续出现在黑名单中的资产数据，而它是有效的资产更新时，白名单非常有用。例如，您可能有一个循环法 DNS 负载均衡器，它配置为循环使用 5 个 IP 地址。资产协调排除规则可能确定多个 IP 地址与同一个 DNS 主机名称相关联表明存在资产增长偏差，系统可将此 DNS 负载均衡器添加至黑名单。为了解决此问题，您可将这个 DNS 主机名添加至资产协调 DNS 白名单。

添加到资产白名单的大量条目

通过准确的资产数据库，可以更轻松地将系统中触发的攻击与网络中的物理资产和虚拟资产相关联。通过将大量条目添加到资产白名单来忽略资产偏差对于构建准确的资产数据库而言并无帮助。请勿添加大量的白名单条目，而应复查资产白名单，以确定导致资产增长偏差的因素，然后确定如何加以修正。

资产白名单的类型

每种类型的身份数据保留在单独的白名单中。下表显示每种身份资产数据的引用集合名称和类型。

表 32. 资产白名单数据的引用集合名称

数据类型	引用集合名称	引用集合类型
IP 地址	资产协调 IPv4 白名单	引用集 [集类型: IP]
DNS 主机名	资产协调 DNS 白名单	引用集 [集类型: ALNIC*]
NetBIOS 主机名	资产协调 NetBIOS 白名单	引用集 [集类型: ALNIC*]
MAC 地址	资产协调 MAC 白名单	引用集 [集类型: ALNIC*]
* ALNIC 是可以适应主机名值和 MAC 地址值的字母数字类型。		

“资产概要文件”页面参数

您可以找到“资产摘要”窗格、“网络接口”窗格、“漏洞”窗格、“服务”窗格、“程序包”窗格、“Windows 补丁”窗格、“属性”窗格、“风险策略”窗格以及“产品”窗格的“资产概要文件”页面参数描述。

本参考资料包含一些表，这些表对**资产概要文件**选项卡的各个窗格中显示的参数进行了描述。

资产概要文件

资产概要文件提供有关网络中每项已知资产的信息，包括正在对每项资产运行哪些服务。

资产概要信息用于进行关联，以帮助减少误报。 例如，如果某个来源尝试渗透资产上运行的特定服务，那么 QRadar 将通过使此攻击与资产概要文件相关联来确定该资产是否易受此攻击伤害。

如果配置了流数据或漏洞评估 (VA) 扫描，那么将自动发现资产概要文件。要使用流数据填充资产概要文件，必须使用双向流。 另外，还可以根据身份事件自动创建资产概要文件。 有关 VA 的更多信息，请参阅 *IBM Security QRadar Vulnerability Assessment Guide*。

有关流源的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

漏洞

您可以使用 QRadar Vulnerability Manager 和第三方扫描程序来确定漏洞。

第三方扫描程序使用外部参考（例如开放式源代码漏洞数据库 (OSVDB)、National Vulnerability Database (NVDB) 和 Critical Watch）来确定和报告已发现的漏洞。第三方扫描程序的示例包括 QualysGuard 和 nCircle ip360。 OSVDB 向每个漏洞分配了唯一的参考标识（OSVDB 标识）。 外部参考向每个漏洞分配了唯一的参考标识。 外部数据参考标识的示例包括通用漏洞与披露 (CVE) 标识和 Bugtraq 标识。 有关扫描程序和漏洞评估的更多信息，请参阅 *IBM Security QRadar Vulnerability Manager User Guide*。

QRadar Vulnerability Manager 是一个组件，您可以单独购买此组件，并使用许可证密钥将其启用。 QRadar Vulnerability Manager 是网络扫描平台，用于提供对网络中应用程序、系统或设备中存在的漏洞的感知。扫描确定漏洞后，您可以搜索并查看漏洞数据、修复漏洞以及重新运行扫描以评估新的风险级别。

启用 QRadar Vulnerability Manager 后，您可以在**漏洞**选项卡上执行漏洞评估任务。在**资产**选项卡中，可以对所选资产运行扫描。

有关更多信息，请参阅 *IBM Security QRadar Vulnerability Manager User Guide*。

“资产”选项卡概述

资产选项卡提供了一个工作空间，您可以从中管理网络资产以及调查资产的漏洞、端口、应用程序、历史记录和其他关联。

通过使用**资产**选项卡，您可以:

- 查看所有已发现的资产。
- 手动添加资产概要文件。
- 搜索特定资产。
- 查看有关已发现的资产的信息。
- 编辑手动添加或发现的资产的资产概要文件。
- 调整误报漏洞。
- 导入资产。
- 打印或导出资产概要文件。
- 发现资产。
- 配置和管理第三方漏洞扫描。
- 启动 QRadar Vulnerability Manager 扫描。

有关导航窗格中的“服务器发现”选项的信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

有关导航窗格中的“VA 扫描”选项的更多信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。

“资产”选项卡列表

“资产概要文件”页面提供了有关标识、IP 地址、资产名称、CVSS 总分、漏洞和服务的信息。

“资产概要文件”页面提供了关于各项资产的以下信息:

表 33. “资产概要文件”页面参数

参数	描述
标识	显示资产的资产标识号。 在您手动添加资产概要文件，或者通过事件、流或漏洞扫描发现资产时，将自动生成资产标识号。
IP 地址	显示资产的最后一个已知 IP 地址。

表 33. “资产概要文件”页面参数 (续)

参数	描述
资产名称	显示资产的给定名称、NetBIOS 名称、DSN 名称或 MAC 地址。 如果这些项未知，那么此字段将显示最后一个已知 IP 地址。 **注**: 这些值按优先顺序显示。 例如，如果资产不具有给定名称，那么将显示聚集 NetBios 名称。 对于自动发现的资产，此字段将自动进行填充，但是，您可以根据需要编辑资产名称。
风险得分	显示下列其中一个通用漏洞评分系统 (CVSS) 得分: • 合并环境 CVSS 总分 • 临时 CVSS 总分 • CVSS 基本总分 • 这些得分按优先顺序显示。 例如，如果合并环境 CVSS 总分不可用，那么将显示临时 CVSS 总分。 CVSS 得分是漏洞严重性的评估指标。 使用 CVSS 得分可以测量某个漏洞与其他漏洞相比值得关注的程度。 CVSS 分数使用下列用户定义参数进行计算: • 潜在间接损害 • 机密性需求 • 可用性需求 • 完整性需求 有关如何配置这些参数的更多信息，请参阅第 111 页的『添加或编辑资产概要文件』。 有关 CVSS 的更多信息，请参阅 http://www.first.org/cvss/。
漏洞数	显示在此资产中发现的非重复漏洞数。 此值还包括活动和被动漏洞数。
服务	显示对此资产运行的非重复第 7 层应用程序数。
最近的用户	显示与此资产相关联的最后一个用户。
最近一次遇到用户时间	显示最后一次遇到与此资产相关联的最后一个用户的时间。

右键单击菜单选项

在“资产”选项卡上右键单击资产将显示菜单，以提供更多事件过滤器信息。

在**资产**选项卡上，可以右键单击资产以访问更多事件过滤器信息。

表 34. 右键单击菜单选项

选项	描述
浏览	**浏览**菜单提供了下列选项: • **按网络查看** - 显示“网络列表”窗口，此窗口将显示所有与选定 IP 地址相关联的网络。 • **查看源摘要** - 显示“攻击列表”窗口，此窗口将显示所有与选定源 IP 地址相关联的攻击。 • **查看目标摘要** - 显示“攻击列表”窗口，此窗口将显示所有与选定目标 IP 地址相关联的攻击。
信息	**信息**菜单提供了下列选项: • **DNS 查找** - 根据 IP 地址搜索 DNS 条目。 • **WHOIS 查找** - 搜索远程 IP 地址的已注册所有者。 缺省 WHOIS 服务器为 whois.arin.net。 • **端口扫描** - 对所选 IP 地址执行网络映射器 (NMAP) 扫描。仅当系统上安装了 NMAP 时，此选项才可用。有关安装 NMAP 的更多信息，请参阅供应商文档。 • **资产概要文件** - 显示资产概要信息。 仅当扫描主动获取了概要文件数据或者流源被动获取此数据时，此菜单选项才可用。 • **搜索事件** - 选择**搜索事件**选项可以搜索与此 IP 地址相关联的事件。 • **搜索流** - 选择“搜索流”选项可以搜索与此 IP 地址相关联的流。
运行漏洞扫描	选择此选项可以对所选资产运行 Vulnerability Manager 扫描。 仅当安装 QRadar Vulnerability Manager 后，才会显示此选项。

查看资产概要文件

您可以从**资产**选项卡上的资产列表中选择并查看资产概要文件。 资产概要文件提供了有关各个概要文件的信息。

关于此任务

资产概要信息通过“服务器发现”自动发现或进行了手动配置。您可以编辑自动生成的资产概要信息。

“资产概要文件”页面提供了有关组织成多个窗格的资产的信息。 要查看某个窗格，您可以单击此窗格上的箭头 **(>)** 以查看更多详细信息，或者从工具栏上的**显示**列表框中选择此窗格。

“资产概要文件”页面工具栏提供了下列功能:

表 35. “资产概要文件”页面工具栏功能

选项	描述
返回到资产列表	单击此选项可以返回到资产列表。
显示	从此列表框中，可以选择要在“资产概要文件”窗格上查看的窗格。 将始终显示“资产摘要”和“网络接口摘要”窗格。 有关各个窗格中显示的参数的更多信息，请参阅资产概要文件页面参数。
编辑资产	单击此选项可以编辑“资产概要文件”。 请参阅第 111 页的『添加或编辑资产概要文件』。
按网络查看	如果此资产与攻击相关联，那么此选项将使您能够查看与此资产相关联的网络列表。 单击**按网络查看**时，将显示“网络列表”窗口。 请参阅第 32 页的『监视按网络分组的攻击』。
查看源摘要	如果此资产是攻击的来源，那么此选项将使您能够查看源摘要信息。 单击**按源摘要查看**时，将显示“攻击列表”窗口。请参阅第 31 页的『监视按源 IP 分组的攻击』。
查看目标摘要	如果此资产是攻击的目标，那么此选项将使您能够查看目标摘要信息。 单击**按目标摘要查看**时，将显示“目标列表”窗口。请参阅第 32 页的『监视按目标 IP 分组的攻击』。
历史记录	单击**历史记录**可以查看此资产的事件历史记录信息。 单击**历史记录**图标时，将显示“事件搜索”窗口，其中预先填充了事件搜索条件: 有需要时，您可以对搜索参数进行定制。 单击**搜索**可以查看事件历史记录信息。
应用程序	单击**应用程序**可以查看此资产的应用程序信息。 单击**应用程序**图标时，将显示“流搜索”窗口，其中预先填充了事件搜索条件。 有需要时，您可以对搜索参数进行定制。 单击**搜索**可以查看应用程序信息。
搜索连接	单击**搜索连接**可以搜索连接。 这将显示“连接搜索”窗口。 仅当您购买了 IBM Security QRadar Risk Manager 并获得此产品的使用授权后，才会显示此选项。 有关更多信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。
查看拓扑	单击**查看拓扑**可以对资产进行进一步调查。 这将显示“当前拓扑”窗口。 仅当您购买了 IBM Security QRadar Risk Manager 并获得此产品的使用授权后，才会显示此选项。 有关更多信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。

表 35. “资产概要文件”页面工具栏功能 (续)

选项	描述
操作	从**操作**列表中，选择**漏洞历史记录**。 仅当您购买了 IBM Security QRadar Risk Manager 并获得此产品的使用授权后，才会显示此选项。 有关更多信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 双击要查看的资产。
4. 使用工具栏上的选项显示资产概要信息的各个窗格。 请参阅编辑资产概要文件。
5. 要研究相关联的漏洞，请在“漏洞”窗格中单击各个漏洞。 请参阅表 10-10
6. 有需要时，编辑资产概要文件。 请参阅编辑资产概要文件。
7. 有需要时，单击**返回到资产列表**以选择并查看另一资产。

添加或编辑资产概要文件

系统自动发现和添加资产概要文件；但是，您可能需要手动添加概要信息

关于此任务

使用“服务器发现”选项来发现资产时，将自动填写部分资产概要文件详细信息。 您可以向资产概要文件手动添加信息，并可以对特定参数进行编辑。

只能对手动输入的参数进行编辑。 系统生成的参数以斜体显示，并且不可编辑。 有需要时，可以将系统生成的参数删除。

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 选择下列其中一个选项:
   - 要添加资产，请单击**添加资产**，然后在**新 IP 地址**字段中输入资产的 IP 地址或 CIDR 范围。
   - 要编辑资产，请双击要查看的资产，然后单击**编辑资产**。
4. 在“MAC 与 IP 地址”窗格中配置参数。配置下列其中一个或多个选项:
   - 单击**新 MAC 地址**图标，然后在对话框中输入 MAC 地址。
   - 单击**新 IP 地址**图标，然后在对话框中输入 IP 地址。
   - 如果列出了**未知 NIC**，那么可以选择此项，然后单击**编辑**图标，并在对话框中输入新 MAC 地址。
   - 从列表中选择 MAC 或 IP 地址，然后单击**编辑**图标，并在对话框中输入新 MAC 地址。
   - 从列表中选择 MAC 或 IP 地址，然后单击**除去**图标。
5. 在“名称与描述”窗格中配置参数。 配置下列其中一个或多个选项:

参数	描述
DNS	选择下列其中一个选项: • 输入 DNS 名称，然后单击**添加**。 • 从列表中选择 DNS 名称，然后单击**编辑**。 • 从列表中选择 DNS 名称，然后单击**除去**。
NetBIOS	选择下列其中一个选项: • 输入 NetBIOS 名称，然后单击**添加**。 • 从列表中选择 NetBIOS 名称，然后单击**编辑**。 • 从列表中选择 NetBIOS 名称，然后单击**除去**。
指定的名称	输入此资产概要文件的名称。
位置	输入此资产概要文件的位置。
描述	输入此资产概要文件的描述。
无线 AP	输入此资产概要文件的无线访问点 (AP)。
无线 SSID	输入此资产概要文件的无线服务集标识 (SSID)。
交换机标识	输入此资产概要文件的交换机标识。
交换机端口标识	输入此资产概要文件的交换机端口标识。

6. 在“操作系统”窗格中配置参数:
   a. 从**供应商**列表框中，选择操作系统供应商。
   b. 从**产品**列表框中，选择资产概要文件的操作系统。
   c. 从**版本**列表框中，选择所选操作系统的版本。
   d. 单击**添加**图标。
   e. 从**覆盖**列表框中，选择下列其中一个选项:
      • **直到下一次扫描为止** - 选择此选项表示扫描程序提供了操作系统信息，并且您可以对此信息进行临时编辑。 如果对操作系统参数进行了编辑，那么扫描程序将在其下次扫描时复原信息。
      • **永久** - 选择此选项表示您希望手动输入操作系统信息，并禁止扫描程序更新此信息。
   f. 从列表中选择操作系统。
   g. 选择操作系统，然后单击**切换覆盖**图标。
7. 在“CVSS 与权重”窗格中配置参数。配置下列其中一个或多个选项:

参数	描述
潜在间接损害	配置此参数可以指示此资产损坏或失窃导致寿命或物理资产损失的可能性。 您还可以使用此参数来指示生产力或收入的经济损失可能性。潜在间接损害增加将导致“CVSS 得分”参数中的计算值增加。 从**潜在间接损害**列表框中，选择下列其中一个选项: • 无 • 低 • 低-中 • 中-高 • 高 • 未定义 配置**潜在间接损害**参数时，**权重**参数将自动更新。
机密性需求	配置此参数可以指示成功渗透的漏洞对此资产的机密性的影响。 机密性影响增加将导致“CVSS 得分”参数中的计算值增加。 从**机密性需求**列表框中，选择下列其中一个选项: • 低 • 中 • 高 • 未定义
可用性需求	配置此参数可以指示成功渗透某个漏洞时，对资产可用性造成的影响。 耗用网络带宽、处理器周期或磁盘空间的攻击可能会影响资产的可用性。 可用性影响增加将导致“CVSS 得分”参数中的计算值增加。 从**可用性需求**列表框中，选择下列其中一个选项: • 低 • 中 • 高 • 未定义

参数	描述
完整性需求	配置此参数可以指示成功渗透某个漏洞时，对资产完整性造成的影响。 完整性指的是信息的可信性以及保证真实性。 完整性影响增加将导致“CVSS 得分”参数中的计算值增加。 从**完整性需求**列表框中，选择下列其中一个选项: • 低 • 中 • 高 • 未定义
权重	从**权重**列表框中，选择此资产概要文件的权重。 范围是 0 - 10。 配置**权重**时，**潜在间接损害**参数将自动更新。

8. 在“所有者”窗格中配置参数。 选择下列其中一个或多个选项:

参数	描述
业务所有者	输入资产的业务所有者姓名。 部门经理是业务所有者的一个示例。 最大长度为 255 个字符。
业务所有者联系人	输入业务所有者的联系信息。 最大长度为 255 个字符。
技术所有者	输入资产的技术所有者。 下面是业务所有者的一个示例: IT 管理员或主管。 最大长度为 255 个字符。
技术所有者联系人	输入技术所有者的联系信息。 最大长度为 255 个字符。
技术用户	在此列表框中，请选择要与此资产概要文件关联的用户名。 另外，还可以使用此参数对 IBM Security QRadar Vulnerability Manager 启用自动漏洞修复。有关自动修复的更多信息，请参阅 *IBM Security QRadar Vulnerability Manager User Guide*。

9. 单击**保存**。

搜索资产概要文件

通过**资产**选项卡上的“资产”页面，可以将搜索参数配置为仅显示要调查的资产概要文件。

关于此任务

访问**资产**选项卡时，将显示“资产”页面，此页面以网络中发现的所有资产进行填充。 要优化此列表，您可以将搜索参数配置为仅显示要调查的资产概要文件。

您可以在“资产搜索”页面中管理资产搜索组。 有关资产搜索组的更多信息， 请参阅资产搜索组。

搜索功能使您能够搜索主机概要信息、资产和身份信息。 身份信息提供了更多关于网络中的日志源的详细信息，其中包括 DNS 信息、用户登录和 MAC 地址。

通过使用资产搜索功能，您可以按外部数据引用搜索资产，以确定部署中是否存在已知的漏洞。

例如:

您接收到一条通知，指出字段中使用了 CVE 标识 CVE-2010-000。 要验证部署中的任何主机是否容易受到此渗透攻击，您可以从搜索参数列表中选择**漏洞外部引用**，选择**CVE**，然后输入

```
2010-000
```

以查看所有容易受该特定 CVE 标识攻击的主机。

注: 有关 OSVDB 的更多信息，请参阅 *http://osvdb.org/*。有关 NVDB 的更多信息，请参阅 *http://nvd.nist.gov/*。

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 在工具栏上，单击**搜索 > 新建搜索**。
4. 选择下列其中一个选项:
   - 要装入先前已保存的搜索，请转至步骤 5。
   - 要创建新搜索，请转至步骤 6。
5. 选择先前已保存的搜索:
   a. 选择下列其中一个选项:
      - 可选。 从**组**列表框中，选择要在**可用的已保存搜索**列表中显示的资产搜索组。
      - 从**可用的已保存搜索**列表中，选择要装入的已保存的搜索。
      - 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。

   b. 单击**装入**。
6. 在“搜索参数”窗格中，定义搜索条件:
   a. 从第一个列表框中，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. 从第二个列表框中，选择要用于搜索的修饰符。
   c. 在输入字段中，输入与搜索参数相关的特定信息。
   d. 单击**添加过滤器**。
   e. 对要添加到搜索条件的过滤器重复这些步骤。
7. 单击**搜索**。

结果

您可以保存资产搜索条件。 请参阅保存资产搜索条件。

保存资产搜索条件

在**资产**选项卡上，可以保存配置的搜索条件，以便将来可以复用该条件。 保存的搜索条件不会到期。

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 执行搜索。
4. 单击**保存条件**。
5. 输入参数的值:

参数	描述
请输入此搜索的名称	输入要分配给此搜索条件的唯一名称。
管理组	单击**管理组**可管理搜索组。 仅当您具有管理许可权时，才会显示此选项。
将搜索分配到组	选中要将这个已保存的搜索分配到的组的复选框。 如果未选择组，那么缺省情况下，这个已保存的搜索将分配到**其他**组。
包括在快速搜索中	选中此复选框可以将此搜索包含在**资产**选项卡工具栏上的**快速搜索**列表框中。
设置为缺省值	选中此复选框可以将此搜索设置为访问**资产**选项卡时的缺省搜索。
与所有人共享	选中此复选框可以与所有用户共享这些搜索需求。

资产搜索组

通过使用“资产搜索组”窗口，可以创建和管理资产搜索组。

借助这些组，您可以在**资产**选项卡中轻松找到已保存的搜索条件。

查看搜索组

使用“资产搜索组”窗口查看组和子组列表。

关于此任务

您可以通过“资产搜索组”窗口查看有关每个组的详细信息，其中包括描述以及最近一次修改组的日期。

所有未分配到组的已保存的搜索位于**其他**组中。

“资产搜索组”窗口显示了每个组的下列参数:

表 36. “资产搜索组”窗口工具栏功能

功能	描述
新建组	要创建新的搜索组，您可以单击**新建组**。 请参阅创建新的搜索组。
编辑	要编辑现有搜索组，您可以单击**编辑**。 请参阅编辑搜索组。
复制	要将已保存的搜索复制到另一搜索组中，您可以单击**复制**。 请参阅将已保存的搜索复制到另一组。
除去	要除去搜索组或者从搜索组中除去已保存的搜索，请选择要除去的项，然后单击**除去**。 请参阅除去组或者从组中除去已保存的搜索。

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 选择**搜索 > 新建搜索**。
4. 单击**管理组**。
5. 查看搜索组。

创建新的搜索组

在“资产搜索组”窗口上，可以创建新的搜索组。

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 选择**搜索 > 新建搜索**。
4. 单击**管理组**。
5. 选择要在其下创建新组的组的文件夹。
6. 单击**新建组**。
7. 在**名称**字段中，输入新组的唯一名称。
8. 可选。 在**描述**字段中，输入描述。
9. 单击**确定**。

编辑搜索组

您可以对搜索组的**名称**和**描述**字段进行编辑。

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 选择**搜索 > 新建搜索**。
4. 单击**管理组**。
5. 选择要编辑的组。

6. 单击**编辑**。
7. 在**名称**字段中输入新名称。
8. 在**描述**字段中输入新描述。
9. 单击**确定**。

将已保存的搜索复制到另一组中

您可以将已保存的搜索复制到另一组中。 另外，还可以将已保存的搜索复制到多个组中。

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 选择**搜索 > 新建搜索**。
4. 单击**管理组**。
5. 选择要复制的已保存的搜索。
6. 单击**复制**。
7. 在“项组”窗口上，选中要将已保存的搜索复制到的组的复选框。
8. 单击**分配组**。

除去组或者从组中除去已保存的搜索

您可以使用**除去**图标从组中除去搜索或除去搜索组。

关于此任务

从某个组中除去已保存的搜索时，已保存的搜索不会从系统中删除。已保存的搜索将从该组中除去，并自动移动至**其他**组。

不能将下列组从系统中除去:

- 资产搜索组
- 其他

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 选择**搜索 > 新建搜索**。
4. 单击**管理组**。
5. 选择要从组中除去的已保存的搜索:
   - 选择要从组中除去的已保存的搜索。
   - 选择要除去的组。

资产概要文件管理任务

通过使用“资产”选项卡，可以删除、导入和导出资产概要文件。

关于此任务

通过使用**资产**选项卡，可以删除、导入和导出资产概要文件。

删除资产

您可以删除特定资产或所有列出的资产概要文件。

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 选择要删除的资产，然后从**操作**列表框中选择**删除资产**。
4. 单击**确定**。

导入资产概要文件

您可以导入资产概要信息。

开始之前

已导入的文件必须是以下格式的 CSV 文件:

```
ip,name,weight,description
```

其中:

- **IP** - 指定任何采用点分十进制格式的有效 IP 地址。 例如: 192.168.5.34。
- **名称** - 指定此资产的名称，其长度不得超过 255 个字符。 逗号在此字段中无效，并且将使导入过程失效。 例如: WebServer01 正确。
- **权重** - 指定数字 0 - 10，该数字指示此资产在网络中的重要性。值 0 表示低重要性，值 10 表示非常高的重要性。
- **描述**- 指定此资产的文本描述，其长度不得超过 255 个字符。 此值是可选的。

例如，以下条目可能包含在 CSV 文件中:

-
```
192.168.5.34,WebServer01,5,Main Production Web Server
```
-
```
192.168.5.35,MailServ01,0,
```

导入过程将已导入的资产概要文件与系统中当前存储的资产概要信息进行合并。

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 从**操作**列表框中，选择**导入资产**。
4. 单击**浏览**以查找并选择要导入的 CSV 文件。
5. 单击**导入资产**以开始导入过程。

导出资产

您可以将列出的资产概要文件导出为扩展标记语言 (XML) 或逗号分隔值 (CSV) 文件。

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 从**操作**列表框中，选择下列其中一个选项:
   - 导出为 XML
   - 导出为 CSV
4. 在状态窗口中查看导出过程的状态。
5. 可选: 如果要在导出正在进行时使用其他选项卡和页面，请单击**完成时发送通知**链接。

   导出完成后，将显示“文件下载”窗口。
6. 在“文件下载”窗口上，选择下列其中一个选项:
   - **打开** - 选择此选项可以所选浏览器打开导出结果。
   - **保存** - 选择此选项可以将结果保存到桌面。
7. 单击**确定**。

研究资产漏洞

“资产概要文件”页面上的“漏洞”窗格显示了资产的已发现的漏洞列表。

关于此任务

您可以双击漏洞来显示更多漏洞详细信息。

“研究漏洞详细信息”窗口提供了以下详细信息:

参数	描述
漏洞标识	指定漏洞的标识。 漏洞标识是由漏洞信息系统 (VIS) 生成的唯一标识。
发布日期	指定在 OSVDB 上发布漏洞详细信息的日期。
名称	指定漏洞的名称。
资产	指定网络中具有此漏洞的资产数。 单击此链接可查看资产列表。
资产（包括异常）	指定网络中具有漏洞异常的资产数。 单击此链接可查看资产列表。
CVE	指定漏洞的 CVE 标识。 CVE 标识由 NVDB 提供。 单击此链接可获取更多信息。 单击此链接时，将在新的浏览器窗口中显示 NVDB Web 站点。
xforce	指定漏洞的 X-Force 标识。 单击此链接可获取更多信息。 单击此链接时，将在新的浏览器窗口中显示 IBM Internet Security Systems Web 站点。

参数	描述
OSVDB	指定漏洞的 OSVDB 标识。 单击此链接可获取更多信息。 单击此链接时，将在新的浏览器窗口中显示 OSVDB Web 站点。
插件详细信息	指定 QRadar Vulnerability Manager 标识。 单击链接可以查看 Oval 定义、Windows 知识库条目或漏洞的 UNIX 建议。 此功能提供了有关 QRadar Vulnerability Manager 如何在补丁扫描过程中检查漏洞详细信息的信息。 您可以使用此功能来确定资产出现漏洞或未出现漏洞的原因。
CVSS 分数库	显示此资产上的漏洞的通用漏洞评分系统 (CVSS) 总分。 CVSS 得分是漏洞严重性的评估指标。使用 CVSS 得分可以测量某个漏洞与其他漏洞相比值得关注的程度。 CVSS 得分使用下列用户定义参数进行计算: • 潜在间接损害 • 机密性需求 • 可用性需求 • 完整性需求 有关如何配置这些参数的更多信息，请参阅第 111 页的『添加或编辑资产概要文件』。 有关 CVSS 的更多信息，请参阅 *http://www.first.org/cvss/*。
影响	显示此漏洞被渗透时可以预期的损害或破坏类型。
CVSS 基本度量	显示用于计算 CVSS 基本分数的度量，其中包括: • 访问向量 • 访问复杂性 • 认证 • 机密性影响 • 完整性影响 • 可用性影响
描述	指定检测到的漏洞的描述。 仅当系统集成了 VA 工具时，此会提供此值。
关注	指定漏洞可能会对网络造成的影响。
解决方案	按照提供的指示信息操作可以解决漏洞。

参数	描述
虚拟修补	显示与此漏洞相关联的虚拟修补信息（如果有）。虚拟修补是针对最近发现的漏洞的短期缓解方案。 此信息根据入侵防御系统 (IPS) 事件而派生。 如果要安装虚拟修补，请参阅 IPS 供应商信息。
参考	显示外部引用列表，其中包括: • **引用类型** - 指定列出的引用的类型，例如咨询 URL 或邮寄列表。 • **URL** - 指定可单击以查看引用的 URL。 单击此链接可获取更多信息。单击此链接时，将在新的浏览器窗口中显示外部资源。
产品	显示与此漏洞相关联的产品列表。 • **供应商** - 指定产品的供应商。 • **产品** - 指定产品名称。 • **版本** - 指定产品的版本号。

过程

1. 单击**资产**选项卡。
2. 在导航菜单中，单击**资产概要文件**。
3. 选择资产概要文件。
4. 在“漏洞”窗格中，单击要调查的漏洞的**标识**或**漏洞**参数值。

第 8 章 图表管理

您可以使用各个图表配置选项来查看数据。

使用**日志活动**和**网络活动**选项卡上的图表，您可以使用各种图表配置选项来查看数据。

图表管理

您可以使用各个图表配置选项来查看数据。

如果您选择时间范围或分组选项来查看数据，那么图表将显示在事件或流列表上方。

在流方式下，不会显示图表。

您可以对图表进行配置，以选择所要绘制的数据。可以彼此独立地配置图表，以便从不同角度显示搜索结果。

图表类型包括:

- 条形图 - 在条形图中显示数据。此选项仅适用于已分组的事件。
- 饼图 - 在饼图中显示数据。此选项仅适用于已分组的事件。
- 表 - 在表中显示数据。此选项仅适用于已分组的事件。
- 时间序列 - 显示交互式折线图，此图表示指定的时间间隔所匹配的记录。有关配置时间序列搜索条件的信息，请参阅时间序列图表概述。

配置图表后，您执行下列操作时，将保留图表配置:

- 使用**显示**列表框更改视图。
- 应用过滤器。
- 保存搜索条件。

执行下列操作时，不会保留图表配置:

- 启动新的搜索。
- 访问快速搜索。
- 在分支窗口中查看已分组结果。
- 保存搜索结果。

注: 如果您使用 Mozilla Firefox Web 浏览器，并且安装了广告拦截器浏览器扩展，那么图表无法显示。要显示图表，必须除去该广告拦截器浏览器扩展。有关更多信息，请参阅浏览器文档。

时间序列图表概述

时间序列图表是一段时间内的活动的图形表示。

图表中显示的峰值和谷值用于描绘大量活动和小量活动。 进行短期和长期数据趋势分析时，时间序列图表非常有用。

通过使用时间序列图表，您可以通过各个视图和透视图访问、浏览以及调查日志或网络活动。

注: 您必须具有相应的角色许可权才能管理和查看时间序列图表。

要显示时间序列图表，您必须创建和保存包含时间序列及分组选项的搜索。 您可以保存多达 100 个时间序列搜索。

保存的缺省时间序列搜索可以从事件或流搜索页面上提供的可用搜索列表中进行访问。

您可以通过**快速搜索**菜单轻松确定已保存的时间序列搜索，这是因为，搜索名称末尾追加了搜索条件中指定的时间范围。

如果搜索参数先前保存的列定义及分组选项搜索相匹配，那么对于搜索结果，可能会自动显示时间序列图表。 对于未保存的搜索条件，如果未自动显示时间序列图表，那么不存在任何先前保存的与搜索参数匹配的搜索条件。 如果发生这种情况，那么必须启用时间序列数据捕获并保存搜索条件。

您可以放大并扫描时间序列图表中的时间线以调查活动。 下表提供可用于查看时间序列图表的功能。

表 37. 时间序列图表功能

功能	描述
更详细地查看数据	通过使用缩放功能，可以调查事件流量的较小时间段。 • 将鼠标指针移动到图表上，然后使用鼠标滚轮放大图表（向上滚动鼠标滚轮）。 • 突出显示要放大的图表区域。 释放鼠标按键时，图表将显示较小的时间段。现在，您可以单击并拖动图表，以扫描图表。 放大时间序列图表时，图表将进行刷新，以显示更小的时间段。
查看较大的数据时间范围	通过使用缩放功能，可以调查更大的时间段或恢复为最大时间范围。 可以使用下列其中一个选项来展开时间范围: • 单击图表左上角的“缩放重置”。 • 将鼠标指针移动到图表上，然后使用鼠标滚轮展开视图（向下滚动鼠标滚轮）。
扫描图表	放大时间序列图表后，可以单击图表，并向左/向右拖动图表以扫描时间线。

图表图注

每个图表都提供了图注，图注是一个可视参考，用于帮助您使图表对象与其表示的参数相关联。

通过使用图注功能部件，可以执行下列操作:

- 将鼠标指针移到图注项或图注色块上方，以查看有关其所表示的参数的更多信息。

- 右键单击图注项，以便对该项进行进一步调查。
- 单击饼图或条形图图注项，以便在图表中隐藏该项。再次单击该图注项将显示隐藏的项。您也可以单击对应的图形项以隐藏和显示该项。
- 如果要从图表显示中除去图注，请单击**图注**或其旁边的箭头。

配置图表

您可以使用配置选项来更改图表类型、要绘图的对象类型，以及图表上显示的对象数。 对于时间序列图表，您还可以选择时间范围并启用时间序列数据捕获。

开始之前

以实时方式（流方式）查看事件或流时，不会显示图表。要显示图表，您必须访问**日志活动**或**网络活动**选项卡，然后选择下列其中一个选项:

- 从**视图**和**显示**列表框中选择选项，然后在工具栏上单击**保存条件**。 请参阅保存搜索条件。
- 在工具栏上，从**快速搜索**列表中选择已保存的搜索。
- 执行分组搜索，然后在工具栏上单击**保存条件**。

如果要配置时间序列图表，请确保已保存的搜索条件进行了分组并指定了时间范围。

关于此任务

数据可以进行累积，以便当您执行时间序列搜索时，数据的高速缓存可用于显示上一时间段的数据。 对所选参数启用时间序列数据捕获后，在“要绘图的值”列表框中，该参数旁边将显示一个星号 (*)。

过程

1. 单击**日志活动**或**网络活动**选项卡。
2. 在“图表”窗格中，单击**配置**图标。
3. 为下列参数配置值:

选项	描述
参数	描述
要绘图的值	在此列表框中，请选择要在图表的 Y 轴上绘制的对象类型。 选项包括搜索参数中包含的所有规范化以及定制事件或流参数。
显示排名靠前的项	在此列表框中，请选择要在图表中查看的对象数。 缺省值为 10。 对任何 10 个以上项进行制图可能导致图表数据不可读。
图表类型	在此列表框中，请选择要查看的图表类型。 如果条形图、饼图或表格图基于时间范围超过 1 小时的已保存的搜索条件，那么必须单击**更新详细信息**来更新图表并填充事件详细信息。

选项	描述
捕获时间序列数据	如果要启用时间序列数据捕获，请选中此复选框。 选中此复选框后，图表功能将开始累积时间序列图表的数据。 缺省情况下，此选项处于禁用状态。 此选项仅在“时间序列”图表上可用。
时间范围	在此列表框中，请选择要查看的时间范围。 此选项仅在“时间序列”图表上可用。

4. 如果您选中了**时间序列**图表选项，并且启用了**捕获时间序列数据**选项，请在工具栏上单击**保存条件**。
5. 如果时间范围大于 1 小时，请单击**更新详细信息**以查看事件或流。

第 9 章 数据搜索

在**日志活动**、**网络活动**和**攻击**选项卡上，您可以使用特定条件来搜索事件、流和攻击。

您可以创建新的搜索，也可以装入先前保存的搜索条件集。您可以选择要在搜索结果中显示的数据列，并可以对其进行组织和分组

事件和流搜索

可以在**日志活动**和**网络活动**选项卡上执行搜索。

执行搜索后，可以保存搜索条件和搜索结果。

搜索满足条件的项

您可以搜索满足搜索条件的数据。

关于此任务

由于对整个数据库执行搜索，因此搜索可能会花费较长的时间，具体取决于数据库的大小。

使用**快速过滤**搜索参数可以搜索与事件有效内容中的文本字符串相匹配的项。

下表描述了您可用于搜索事件和流数据的搜索选项:

表 38. 搜索选项

选项	描述
组	选择要在**可用的已保存搜索**列表中查看的事件搜索组或流搜索组。
输入已保存的搜索或者从列表中进行选择	输入已保存的搜索的名称或关键字，以过滤**可用的已保存搜索**列表。
可用的已保存搜索	除非您使用**组或输入已保存的搜索**或者**从列表进行选择**选项对此列表应用了过滤器，否则此列表将显示所有可用的搜索。 您可以在此列表中选择已保存的搜索以进行显示或编辑。
搜索	“搜索”页面的多个窗格中提供了**搜索**图标。 如果您已完成配置搜索并希望查看结果，那么可以单击“搜索”。
包括在快速搜索中	选中此复选框可以将此搜索包含在**快速搜索**菜单中。
包括在仪表板中	选中此复选框可以将已保存的搜索中的数据保存在**仪表板**选项卡中。 有关**仪表板**选项卡的更多信息，请参阅仪表板管理。 **注**: 仅当对搜索进行了分组时，才会显示此参数。

表 38. 搜索选项 (续)

选项	描述
设置为缺省值	选中此复选框可以将此搜索设置为缺省搜索。
与所有人共享	选中此复选框可以与所有其他用户共享此搜索。
实时（流式方法）	以流方式显示结果。 有关流方式的更多信息，请参阅查看流式事件。 **注**: 启用实时（流式方法）后，您将不能对搜索结果进行分组。 如果在“列定义”窗格中选择了任何分组选项，那么将打开一条错误消息。
上次时间间隔（自动刷新）	以自动刷新方式显示搜索结果。 在自动刷新模式下，**日志活动**和**网络活动**选项卡每分钟刷新一次，以显示最新信息。
最近	为搜索选择预定义的时间范围。选择此选项后，必须从列表框中选择时间范围选项。
特定的时间间隔	为搜索选择定制时间范围。选择此选项后，必须从**开始时间**和**结束时间**日历中选择日期和时间范围。
数据累积	仅当装入已保存的搜索时，才会显示此窗格。 对于和很多其他已保存的搜索和报告共享的累积数据，启用针对此数据的唯一计数可能会降低系统性能。 装入已保存的搜索时，此窗格将显示下列选项: • 如果未针对这个已保存的搜索累积任何数据，那么将显示以下参考消息: 未针对此搜索累积任何数据。 • 如果针对这个已保存的搜索累积了数据，那么将显示下列选项: – **列** - 单击或将鼠标悬停在此链接上方时，将打开累积数据的列的列表。 – **启用唯一计数/禁用唯一计数** - 通过此链接，您可以启用或禁用搜索结果以显示一段时间内的唯一事件和流计数，而不是显示平均计数。单击**启用唯一计数**链接后，将打开一个对话框，此对话框指示哪些已保存的搜索和报告共享累积数据。
当前过滤器	此列表显示应用于此搜索的过滤器。 用于添加过滤器的选项位于**当前过滤器**列表上方。
完成搜索后保存结果	选中此复选框可以保存并命名搜索结果。
显示	选择此列表可以指定一个预定义列，此列设置为在搜索结果中显示。

表 38. 搜索选项 (续)

选项	描述
输入列或从列表进行选择	您可以使用此字段过滤“可用列”列表中列出的列。 输入要查找的列的名称，或者输入某个关键字以显示列名称列表。 例如，输入 Device 可以显示列名称中包含 Device 的列的列表。
可用列	此列表显示可用列。 当前已用于这个已保存的搜索的列将在**列**列表中突出显示。
添加和除去列图标（顶部集）	使用顶部的图标集可以定制**分组依据**列表。 • **添加列** - 从**可用列**列表中选择一个或多个列，然后单击**添加列**图标。 • **除去列** - 从**分组依据**列表中选择一个或多个列，然后单击**除去列**图标。
添加和除去列图标（底部集）	使用底部的图标集合可以定制**列**列表。 • **添加列** - 从“可用列”列表中选择一个或多个列，然后单击**添加列**图标。 • **除去列** - 从“列”列表中选择一个或多个列，然后单击**除去列**图标。
分组依据	此列表指定已保存的搜索对结果进行分组的依据。 使用下列选项可以进一步地定制“分组依据”列表: • 向上移动 - 选择一个列，然后使用**向上移动**图标在优先级列表中向上移动此列。 • 向下移动 - 选择一个列，然后使用**向下移动**图标在优先级列表中向下移动此列。 优先级列表指定结果的分组顺序。 搜索结果按**分组依据**列表中的第一列进行分组，然后按此列表中的下一列进行分组。
列数	指定选定的要搜索的列。可以从**可用列**列表中选择多列。可以使用下列选项进一步地定制**列**列表: • **向上移动** - 在优先级列表中向上移动所选列。 • **向下移动** - 在优先级列表中向下移动所选列。 如果列类型是数字或基于时间，并且**分组依据**列表中存在条目，那么列将包含一个列表框。使用此列表框可以选择希望对列执行的分组方式。 如果列类型是组，那么列将包含一个列表框，用于选择要针对组提供的级别数。
排序依据	从第一个列表框中，选择要作为搜索结果的排序依据的列。 然后，从第二个列表框中，选择搜索结果的显示顺序。选项包括**降序**和**升序**。

表 38. 搜索选项 (续)

选项	描述
结果限制	您可以在“编辑搜索”窗口中指定搜索返回的行数。 另外，**结果限制**字段还将显示在“结果”窗口中。 • 对于已保存的搜索，限制存储在已保存的搜索中，并在装入搜索时重新应用。 • 在具有行限制的搜索结果中根据某列执行排序时，排序将在数据网格中显示的有限行内完成。 • 对于启用了时间序列图表的分组依据搜索，行限制仅适用于数据网格。 时间序列图表中的**排名前 N 位**下拉列表仍然控制图表中绘制的时间序列数。

过程

1. 选择下列其中一个选项:
   - 要搜索事件，请单击**日志活动**选项卡。
   - 要搜索流，请单击**网络活动**选项卡。
2. 从**搜索**列表框中，选择**新建搜索**。
3. 要选择先前已保存的搜索，请完成下列步骤:
   a. 选择下列其中一个选项: 从"可用的已保存搜索"列表中，选择要装入的已保存搜索。 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。
   b. 单击**装入**。
   c. 在“编辑搜索”窗格中，选择要用于此搜索的选项。 请参阅表 1。
4. 要创建搜索，请在“时间范围”窗格中，选择要针对此搜索捕获的时间范围选项。
5. 可选。 在“数据累积”窗格中，启用唯一计数:
   a. 单击**启用唯一计数**。
   b. 在“警告”窗口上，阅读警告消息，然后单击**继续**。 有关启用唯一计数的更多信息，请参阅表 1。
6. 在“搜索参数”窗格中，定义搜索条件:
   a. 从第一个列表框中，选择要搜索的参数。 例如，设备、源端口或事件名称。
   b. 从第二个列表框中，选择要用于搜索的修饰符。
   c. 在输入字段中，输入与搜索参数相关的特定信息。
   d. 单击**添加过滤器**。
   e. 对要添加到搜索条件的各个过滤器重复步骤 a 到 d。
7. 可选。 要在搜索完成后自动保存搜索结果，请选中**完成搜索后保存结果**复选框，然后输入已保存的搜索的名称。
8. 在“列定义”窗格中，定义要用于查看结果的列和列布局:
   a. 从**显示**列表框中，选择设置为与此搜索相关联的预配置列。
   b. 单击**高级视图定义**旁边的箭头以显示高级搜索参数。

c. 定制要在搜索结果中显示的列。请参阅表 1。

d. 可选。 在**结果限制**字段中，输入希望搜索返回的行数。

9. 单击**过滤**。

结果

右上角中将显示**正在进行中（<percent> 完成百分比）**状态。

.

查看部分搜索结果时，搜索引擎将在后台工作以完成搜索，并刷新部分结果以更新视图。

搜索完成后，右上角将显示**已完成**状态。

保存搜索条件

您可以保存已配置的搜索条件，以便在报告之类的其他组件中复用此条件以及使用已保存的搜索条件。 保存的搜索条件不会到期。

关于此任务

如果您为搜索指定了时间范围，那么指定的时间范围将追加到搜索名称后面。 例如，名为“渗透（按来源排列）”且时间范围为过去 5 分钟的保存的搜索将变成“渗透（按来源排列）- 过去 5 分钟”。

如果您更改了在先前保存的搜索中设置的列，然后使用同一名称保存搜索条件，那么时间序列图表的先前累积将会丢失。

过程

1. 选择下列其中一个选项:
   - 单击**日志活动**选项卡。
   - 单击**网络活动**选项卡。
2. 执行搜索。
3. 单击**保存条件**。
4. 输入参数的值:

选项	描述
参数	描述
搜索名称	输入要分配给此搜索条件的唯一名称。
将搜索分配到组	选中要将这个已保存的搜索分配到的组的复选框。 如果未选择组，那么缺省情况下，这个已保存的搜索将分配到“其他”组。 有关更多信息，请参阅管理搜索组。
管理组	单击**管理组**可以管理搜索组。 有关更多信息，请参阅管理搜索组。

选项	描述
时间范围选项:	选择下列其中一个选项: • **实时（流式方法）**- 选择此选项将在流方式下过滤搜索结果。 • **上次时间间隔（自动刷新）** - 选择此选项将在自动刷新方式下过滤搜索结果。 **日志活动**和**网络活动**选项卡每分钟刷新一次，以显示最新的信息。 • **最近** - 选择此选项，然后从此列表框中选择要执行过滤的时间范围。 • **特定的时间间隔** - 选择此选项，然后从日历中选择要执行过滤的日期和时间范围。
包括在快速搜索中	选中此复选框可以将此搜索包含在工具栏上的**快速搜索**列表框中。
包括在仪表板中	选中此复选框可以将已保存的搜索中的数据保存在**仪表板**选项卡中。 有关**仪表板**选项卡的更多信息，请参阅仪表板管理。 **注:** 仅当对搜索进行了分组时，才会显示此参数。
设置为缺省值	选中此复选框可以将此搜索设置为缺省搜索。
与所有人共享	选中此复选框可以与所有用户共享这些搜索需求。

5. 单击**确定**。

调度搜索

使用“调度搜索”选项可以调度搜索并查看结果。

您可以对在白天或夜晚的特定时间运行的搜索进行调度。

示例:
如果将搜索调度为在夜晚运行，那么您可以在早晨进行调查。 与报告不同，您可以选择对搜索结果进行分组并执行进一步的调查。 您可以在网络组中对许多失败的登录进行搜索。 如果结果通常为 10 且搜索结果为 100，那么您可以对搜索结果进行分组以方便调查。要查看哪个用户的登录失败次数最多，您可以按用户名分组。 您可以继续执行进一步的调查。

您可以从**报告**选项卡调度对事件或流的搜索。您必须选择先前保存的一组搜索条件以进行调度。

1. 创建报告

   在**报告向导**窗口中指定以下信息:
   - 图表类型为事件/日志或流。
   - 该报告基于保存的搜索。
   - 生成攻击。

     您可以选择**创建单个攻击**选项或**将结果添加到现有攻击**选项。

您还可以生成手动搜索。

2. 查看搜索结果

您可以从**攻击**选项卡查看调度搜索的结果。

- 调度搜索攻击由**攻击类型**列标识。

  如果您创建单个攻击，那么每当报告运行时将生成攻击。 如果将保存的搜索结果添加到现有攻击，那么在报告首次运行时创建攻击。 后续报告运行附加到此攻击。 如果未返回结果，那么系统不会附加或创建攻击。

- 要在“攻击摘要窗口中查看最近的搜索结果，请双击攻击列表中的调度搜索攻击。 要查看所有调度搜索运行的列表，请单击**最后 5 个搜索结果**窗格中的**搜索结果**。

您可以向用户分配调度搜索攻击。

相关任务:

第 127 页的『搜索满足条件的项』
您可以搜索满足搜索条件的数据。

第 37 页的『将攻击分配给用户』
通过使用**攻击**选项卡，可以将攻击分配给用户以进行调查。

高级搜索选项

使用**高级搜索**字段可以输入 Ariel Query Language (AQL)，此语言用于指定您需要的字段以及希望如何对这些字段进行分组以运行查询。

高级搜索字段具有自动填写和语法突出显示功能。

使用自动填写和语法突出显示功能可以帮助创建查询。有关受支持的 Web 浏览器的信息，请参阅第 6 页的『支持 Web 浏览器』

访问高级搜索

从位于**网络活动**和**日志活动**选项卡中的**搜索**工具栏访问**高级搜索**选项以输入 AQL 查询。

从**搜索**工具栏上的列表框中选择**高级搜索**。

通过以下步骤来展开**高级搜索**字段:

1. 拖动位于字段右侧的展开图标。
2. 按 Shift + Enter 键以前进至下一行。
3. 按 Enter 键。

您可以右键单击搜索结果中的任何值并对该值进行过滤。

双击搜索结果中的任何行可以查看更多详细信息。

包括 AQL 搜索在内的所有搜索将包含在审计日志中。

AQL 搜索字符串示例

下表提供了 AQL 搜索字符串的示例。

表 39. AQL 搜索字符串的示例

描述	示例
从事件中选择缺省列。 从流中选择缺省列。	SELECT * FROM events SELECT * FROM flows
选择特定列。	SELECT sourceip, destinationip FROM events
选择特定列并对结果进行排序。	SELECT sourceip, destinationip FROM events ORDER BY destinationip
运行聚集搜索查询。	SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip
在 SELECT 子句中运行函数调用。	SELECT CATEGORYNAME(category) AS namedCategory FROM events
使用 WHERE 子句过滤搜索结果。	SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1
搜索触发特定规则的事件，此规则基于规则名称或规则名称中的部分文本。	SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'
通过用双引号将字段名称引起来，引用包含特殊字符（例如，算数字符或空格）的字段名称。	SELECT sourceip, destinationip, ″+field/name+″ FROM events WHERE ″+field/name+″ LIKE '%test%'

下表提供 X-Force 的 AQL 搜索字符串的示例。

表 40. X-Force 的 AQL 搜索字符串示例

描述	示例
使用置信度值根据 X-Force 类别检查 IP 地址。	select * from events where XFORCE_IP_CONFIDENCE('Spam',sourceip)>3
搜索与 URL 关联的 X-Force URL 类别。	select url, XFORCE_URL_CATEGORY(url) as myCategories from events where XFORCE_URL_CATEGORY(url) IS NOT NULL
检索与 IP 关联的 X-Force IP 类别。	select sourceip, XFORCE_IP_CATEGORY (sourceip) as IPcategories from events where XFORCE_IP_CATEGORY(sourceip) IS NOT NULL

有关函数、搜索字段和运算符的更多信息，请参阅《*Ariel 查询语言指南*》。

AQL 搜索字符串示例

使用 Ariel Query Language (AQL) 可以从 Ariel 数据库中的事件、流以及 simarc 表中检索特定字段。

注: 构建 AQL 查询时，如果将包含单引号的文本从任何文档复制粘贴到 IBM Security QRadar 中，那么将无法解析此查询。变通方法为可将此文本粘贴到 QRadar 中，并重新输入单引号，或者可以从 IBM Knowledge Center 复制粘贴此文本。

报告帐户用途

不同的用户社区会遇到不同的威胁并具有不同的用途指标。

使用参考数据可以报告多个用户属性，例如部门、位置或经理。

您可以使用外部参考数据。

以下查询会从用户的登录事件中返回用户的相关元数据信息。

```
SELECT
REFERENCETABLE('user_data','FullName',username) as 'Full Name',
REFERENCETABLE('user_data','Location',username) as 'Location',
REFERENCETABLE('user_data','Manager',username) as 'Manager',
UNIQUECOUNT(username) as 'Userid Count',
UNIQUECOUNT(sourceip) as 'Source IP Count',
COUNT(*) as 'Event Count'
FROM events
WHERE qidname(qid) ILIKE '%logon%'
GROUP BY 'Full Name', 'Location', 'Manager'
LAST 1 days
```

跨多个帐户标识的洞察

在此示例中，各个用户在网络中有多个帐户。 组织需要关于用户活动的单一视图。

使用参考数据可以将本地用户标识映射到全局标识。

以下查询将返回全局标识对标记为“可疑”的事件使用的用户帐户。

```
SELECT
REFERENCEMAP('GlobalID Mapping',username) as 'Global ID',
REFERENCETABLE('user_data','FullName', 'Global ID') as 'Full Name',
UNIQUECOUNT(username),
COUNT(*) as 'Event count'
FROM events
WHERE RULENAME(creEventlist) ILIKE '%suspicious%'
GROUP BY 'Global ID'
LAST 1 days
```

以下查询将显示由全局标识完成的活动。

```
SELECT
QIDNAME(qid) as 'Event name',
starttime as 'Time',
sourceip as 'Source IP', destinationip as 'Destination IP',
username as 'Event Username',
REFERENCEMAP('GlobalID_Mapping', username)as 'Global User'
FROM events
WHERE 'Global User' = 'John Doe'
LAST 1 days
```

标识可疑的长期信标

许多威胁使用命令和控件在数天、数周和数月的时间内定期进行通信。

高级搜索可以随时间推移识别连接模式。 例如，您可以在 IP 地址之间或 IP 地址与地理位置之间查询每天/周/月的一致、短期、低容量连接及连接数。

使用 IBM Security QRadar REST API 可以生成工具或填充引用集或引用表。

以下查询将检测每小时发出的信标的潜在实例。

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'hh')) as 'different hours',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection = 'L2R'
GROUP BY sourceip, destinationip
HAVING 'different hours' > 20
AND 'total flows' < 25
LAST 24 hours
```

提示: 您可以修改此查询以处理代理日志及其他事件类型。

以下查询将检测每天发出的信标的潜在实例。

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'dd'))as 'different days',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection='L2R'
GROUP BY sourceip, destinationip
HAVING 'different days' > 4
AND 'total flows' < 14
LAST 7 days
```

以下查询将检测源 IP 和目标 IP 之间每天发出的信标。 每天发信标的时间不同。 信标之间流逝的时间较短。

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG( hourofday*hourofday) - (AVG(hourofday)^2))as variance,
COUNT(*) as 'total flows'
FROM flows
GROUP BY sourceip, destinationip
HAVING variance < 01 and 'total flows' < 10
LAST 7 days
```

以下查询将使用代理日志事件来检测每天发送到域的信标。 每天发信标的时间不同。 信标之间流逝的时间较短。

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG(hourofday*hourofday) - (AVG(hourofday)^2)) as variance,
COUNT(*) as 'total events'
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist) ILIKE '%proxy%'
GROUP BY url_domain
HAVING variance < 0.1 and 'total events' < 10
LAST 7 days
```

url_domain 属性是代理日志中的定制属性。

外部威胁情报

与外部威胁情报相关联的使用情况和安全性可以提供重要的威胁指标。

高级搜索可以交叉引用外部威胁情报指标及其他安全事件及使用情况数据。

此查询将显示如果对数天、数周或数月的外部威胁数据进行概要分析，以确定资产和帐户的风险级别并划分优先级。

```
Select
REFERENCETABLE('ip_threat_data','Category',destinationip) as 'Category',
REFERENCETABLE('ip_threat_data','Rating', destinationip) as 'Threat Rating',
UNIQUECOUNT(sourceip) as 'Source IP Count',
UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 days
```

资产情报和配置

威胁和用途指标随资产类型、操作系统、漏洞情形、服务器类型、分类及其他参数的不同而有所变化。

在此查询中，高级搜索和资产模型提供了对位置的操作洞察。

Assetproperty 函数用于从资产中检索属性值，这使您可以在结果中包含资产数据。

```
SELECT
ASSETPROPERTY('Location',sourceip) as location,
COUNT(*) as 'event count'
FROM events
GROUP BY location
LAST 1 days
```

以下查询显示了如何在资产模型中使用高级搜索和用户身份跟踪。

AssetUser 函数用于从资产数据库中检索用户名。

```
SELECT
APPLICATIONNAME(applicationid) as App,
ASSETUSER(sourceip, now()) as srcAssetUser,
COUNT(*) as 'Total Flows'
FROM flows
WHERE srcAssetUser IS NOT NULL
GROUP BY App, srcAssetUser
ORDER BY 'Total Flows' DESC
LAST 3 HOURS
```

Network LOOKUP 函数

您可以使用 **Network LOOKUP** 函数检索与 IP 地址关联的网络名。

```
SELECT NETWORKNAME(sourceip) as srcnet,
NETWORKNAME(destinationip) as dstnet
FROM events
```

Rule LOOKUP 函数

您可以使用 **Rule LOOKUP** 函数按规则标识检索规则名称。

```
SELECT RULENAME(123) FROM events
```

以下查询将返回触发特定规则名称的事件。

```
SELECT * FROM events
WHERE RULENAME(creEventList) ILIKE '%my rule name%'
```

全文搜索

您可以使用 TEXT SEARCH 运算符通过**高级搜索**选项来执行全文搜索。

在此示例中，存在许多有效内容中含有单词“firewall”的事件。 您可以使用**日志活动**选项卡上的**快速过滤**选项和**高级搜索**选项来搜索这些事件。

- 要使用**快速过滤**选项，请在**快速过滤**框中输入以下文本: `'firewall'`
- 要使用**高级搜索**选项，请在**高级搜索**框中输入以下查询:

```
SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'
```

定制属性

您可以在使用**高级搜索**选项时访问事件和流的定制属性。

以下查询使用定制属性“MyWebsiteUrl”按特定 Web URL 对事件进行排序:

```
SELECT "MyWebsiteUrl", * FROM events ORDER BY "MyWebsiteUrl"
```

相关概念:

『快速过滤搜索选项』
通过输入使用简单单词或短语的文本搜索字符串来搜索事件和流有效内容。

相关任务:

第 156 页的『创建基于正则表达式的定制属性』
您可以创建基于正则表达式的定制属性，用于将事件或流有效内容与正则表达式匹配。

快速过滤搜索选项

通过输入使用简单单词或短语的文本搜索字符串来搜索事件和流有效内容。

您可以从以下位置对搜索进行过滤:

日志活动工具栏和网络活动工具栏

从**搜索**工具栏上的列表框中选择**快速过滤**以输入文本搜索字符串。单击**快速过滤**图标以便将**快速过滤**应用于事件或流的列表。

添加过滤器对话框

单击**日志活动**或**网络活动**选项卡上的**添加过滤器**图标。

选择**快速过滤**作为过滤参数，然后输入文本搜索字符串。

流搜索页面

将快速过滤添加到过滤器列表中。

以实时（流式方法）或最近时间间隔方式查看**流**时，您只能在**快速过滤**字段中输入简单单词或短语。查看时间范围内的**事件**或**流**时，请遵循以下语法准则:

表 41. 快速过滤语法准则

描述	示例
包含您期望在有效内容中找到的任何纯文本。	`Firewall`
通过在双引号中包含多个项来搜索准确的短语。	`"Firewall deny"`

表 41. 快速过滤语法准则 (续)

描述	示例
包含单字符和多字符通配符。搜索项不能以通配符开头。	`F?rewall 或 F??ew*`
使用逻辑表达式（例如，AND、OR 和 NOT）对项进行分组。语法和运算符必须使用大写才能被识别为逻辑表达式而不是搜索项。	`(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)`
创建包含 NOT 逻辑表达式的搜索条件时，必须至少包含另一种逻辑表达式类型，否则不会返回任何结果。	`(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`
在下列字符前面添加反斜杠以指示该字符是搜索项的组成部分：`+ - && || ! () {} [] ^ " ~ * ? : \`。	`"%PIX\-5\-304001"`

搜索项从有效内容单词或短语中的第一个字符开始依次进行匹配。搜索项 `user` 与 `user_1` 和 `user_2` 匹配，但与下列短语不匹配：`ruser`、`myuser` 或 `anyuser`。

快速过滤搜索使用英语语言环境。*语言环境*设置标识语言或地理区域并确定格式约定，如整理规则、大小写转换、字符分类、消息语言、日期和时间表示以及数字表示。

语言环境由您的操作系统设置。您可以配置 QRadar 以覆盖操作系统语言环境设置。例如，您可以将语言环境设置为**英语**并且可以将 QRadar Console 设置为 **Italiano（意大利语）**。

如果在快速过滤搜索查询中使用 Unicode 字符，可能会返回意外的搜索结果。

如果选择非英语语言环境，您可以使用 QRadar 中的“高级搜索”选项来搜索事件和有效内容数据。

相关概念:

第 127 页的第 9 章，『数据搜索』
在**日志活动**、**网络活动**和**攻击**选项卡上，您可以使用特定条件来搜索事件、流和攻击。

第 133 页的『高级搜索选项』
使用**高级搜索**字段可以输入 Ariel Query Language (AQL)，此语言用于指定您需要的字段以及希望如何对这些字段进行分组以运行查询。

第 134 页的『AQL 搜索字符串示例』
使用 Ariel Query Language (AQL) 可以从 Ariel 数据库中的事件、流以及 simarc 表中检索特定字段。

相关任务:

第 15 页的『更新用户首选项』
在主要 IBM Security QRadar SIEM 用户界面中，您可以设置用户首选项，例如，语言环境。

攻击搜索

您可以使用特定条件来搜索攻击，以便在结果列表中显示与该搜索条件匹配的攻击。

您可以创建新的搜索，也可以装入先前保存的搜索条件集。

在“我的攻击”和“所有攻击”页面上搜索攻击

在**攻击**选项卡的“我的攻击”和“所有攻击”页面上，可以搜索满足条件的攻击。

关于此任务

下表对可以用来在**我的攻击**和**所有攻击**页面上搜索攻击数据的搜索选项进行了描述。

有关类别的信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

表 42. “我的攻击”和“所有攻击”页面搜索选项

选项	描述
组	通过此列表框，您可以选择要在**可用的已保存搜索**列表中查看的攻击搜索组。
输入已保存的搜索或者从列表中进行选择	通过此字段，您可以输入已保存的搜索的名称或关键字，以过滤**可用的已保存搜索**列表。
可用的已保存的搜索	除非您使用“组”或者“输入已保存的搜索或从**列表**进行选择”选项对此列表应用了过滤器，否则此列表将显示所有可用的搜索。 您可以在此列表中选择已保存的搜索以进行显示或编辑。
所有攻击	通过此选项，您可以搜索所有攻击，而与时间范围无关。
最近	通过此选项，您可以选择过滤时要使用的预定义时间范围。 选择此选项后，必须从列表框中选择时间范围选项。
特定时间间隔	通过此选项，您可以为搜索配置定制时间范围。 选择此选项后，您必须选择下列其中一个选项。 • **开始日期的范围** - 选中此复选框可以搜索在特定时间段内启动的攻击。选中此复选框后，请使用列表框来选择要搜索的日期。 • **最后一个事件/流范围** - 选中此复选框可以搜索特定时间段内针对其发生最近已检测事件的攻击。选中此复选框后，请使用列表框来选择要搜索的日期。
搜索	“搜索”页面的多个窗格中提供了**搜索**图标。 如果您已完成配置搜索并希望查看结果，那么可以单击**搜索**。
攻击标识	在此字段中，可以输入要搜索的攻击标识。
描述	在此字段中，可以输入要搜索的描述。
指定给用户	从此列表框中，可以选择要搜索的用户名。

表 42. “我的攻击”和“所有攻击”页面搜索选项 (续)

选项	描述
方向	从此列表框中，可以选择要搜索的攻击方向。选项包括: • 本地到本地 • 本地到远程 • 远程到本地 • 远程到远程 • 从本地到远程或本地 • 从远程到远程或本地
源 IP	在此字段中，可以输入要搜索的源 IP 地址或 CIDR 范围。
目标 IP	在此字段中，可以输入要搜索的目标 IP 地址或 CIDR 范围。
规模	从此列表框中，可以指定规模，然后选择仅显示规模等于、小于或大于配置值的攻击。 范围是 0 - 10。
严重性	从此列表框中，可以指定严重性，然后选择仅显示严重性等于、小于或大于配置值的攻击。范围是 0 - 10。
可信性	从此列表框中，可以指定可信性，然后选择仅显示可信性等于、小于或大于配置值的攻击。范围是 0 - 10。
相关性	从此列表框中，可以指定相关性，然后选择仅显示相关性等于、小于或大于配置值的攻击。范围是 0 - 10。
包含用户名	在此字段中，可以输入一个正则表达式 (regex) 语句，以搜索包含特定用户名的攻击。 定义定制正则表达式模式时，请遵守 Java™ 编程语言定义的正则表达式规则。 有关更多信息，您可以参阅 Web 上提供的正则表达式教程。
源网络	从此列表框中，可以选择要搜索的源网络。
目标网络	从此列表框中，可以选择要搜索的目标网络。
高级别类别	从此列表框中，可以选择要搜索的高级别类别。.
低级别类别	从此列表框中，可以选择要搜索的低级别类别。
排除	通过此窗格中的选项，您可以将攻击从搜索结果中排除。 选项包括: • 处于活动状态的攻击 • 隐藏的攻击 • 关闭的攻击 • 处于非活动状态的攻击 • 受保护的攻击

表 42. “我的攻击”和“所有攻击”页面搜索选项 (续)

选项	描述
关闭（按用户排列）	仅当“排除”窗格中取消选中了**关闭的攻击**复选框时，才会显示此参数。 从此列表框中，可以选择要在关闭的攻击中搜索的用户名，或者选择 Any 以显示所有关闭的攻击。
关闭原因	仅当“排除”窗格中取消选中了**关闭的攻击**复选框时，才会显示此参数。 从此列表框中，可以选择要在关闭的攻击中进行搜索的原因，或者选择 **Any** 以显示所有关闭的攻击。
事件数	从此列表框中，可以指定事件计数，然后选择仅显示事件计数等于、小于或大于配置值的攻击。
流	从此列表框中，可以指定流计数，然后选择仅显示流计数等于、小于或大于配置值的攻击。
事件/流总数	在此列表框中，您可以指定事件和流总计数，然后选择仅显示事件和流总计数等于、小于或大于所配置值的攻击。
目标	从此列表框中，可以指定目标 IP 地址计数，然后选择仅显示目标 IP 地址计数等于、小于或大于配置值的攻击。
日志源组	从此列表框中，可以选择要搜索的日志源所在的日志源组。 **日志源**列表框显示了所有分配到所选日志源组的日志源。
日志源	从此列表框中，可以选择要搜索的日志源。
规则组	从此列表框中，可以选择要搜索的添加内容的规则所在的规则组。 **规则**列表框显示了所有分配到所选规则组的规则。
规则	从此列表框中，可以选择要搜索的添加内容的规则。
攻击类型	从此列表框中，可以选择要搜索的攻击类型。有关**攻击类型**列表框中的选项的更多信息，请参阅表 2。

下表对**攻击类型**列表框中提供的选项进行了描述:

表 43. “攻击类型”选项

攻击类型	描述
不限	此选项用于搜索所有攻击源。
源 IP	要搜索具有特定源 IP 地址的攻击，您可以选择此选项，然后输入要搜索的源 IP 地址。
目标 IP	要搜索具有特定目标 IP 地址的攻击，您可以选择此选项，然后输入要搜索的目标 IP 地址。

表 43. “攻击类型”选项 (续)

攻击类型	描述
事件名称	要搜索具有特定事件名称的攻击，您可以单击**浏览**图标以打开“事件浏览器”，然后选择要搜索的事件名称 (QID)。 您可以使用下列其中一个选项搜索特定 QID: • 要按类别搜索 QID，请选中**按类别浏览**复选框，然后从列表框中选择高级别或低级别类别。 • 要按日志源类型搜索 QID，请选中**按日志源类型浏览**复选框，然后从**日志源类型**列表框中选择日志源类型。 • 要按日志源类型搜索 QID，请选中**按日志源类型浏览**复选框，然后从**日志源类型**列表框中选择日志源类型。 • 要按名称搜索 QID，请选中 **QID 搜索**复选框，然后在 **QID/名称**字段中输入名称。
用户名	要搜索具有特定用户名的攻击，您可以选择此选项，然后输入要搜索的用户名。
源 MAC 地址	要搜索具有特定源 MAC 地址的攻击，您可以选择此选项，然后输入要搜索的源 MAC 地址。
目标 MAC 地址	要搜索具有特定目标 MAC 地址的攻击，您可以选择此选项，然后输入要搜索的目标 MAC 地址。
日志源	从**日志源组**列表框中，可以选择要搜索的日志源所在的日志源组。 **日志源**列表框显示了所有分配到所选日志源组的日志源。 从**日志源**列表框中，选择要搜索的日志源。
主机名	要搜索具有特定主机名的攻击，您可以选择此选项，然后输入要搜索的主机名。
源端口	要搜索具有特定源端口的攻击，您可以选择此选项，然后输入要搜索的源端口。
目标端口	要搜索具有特定目标端口的攻击，您可以选择此选项，然后输入要搜索的目标端口。
源 IPv6	要搜索具有特定源 IPv6 地址的攻击，您可以选择此选项，然后输入要搜索的源 IPv6 地址。
目标 IPv6	要搜索具有特定目标 IPv6 地址的攻击，您可以选择此选项，然后输入要搜索的目标 IPv6 地址。
源 ASN	要搜索具有特定源 ASN 的攻击，您可以从**源 ASN** 列表框中选择源 ASN。
目标 ASN	要搜索具有特定目标 ASN 的攻击，您可以从**目标 ASN** 列表框中选择目标 ASN。

表 43. “攻击类型”选项 (续)

攻击类型	描述
规则	要搜索与特定规则相关联的攻击，您可以从**规则组**列表框中选择要搜索的规则所在的规则组。 **规则组**列表框显示了所有分配到所选规则组的规则。 从**规则**列表框中，可以选择要搜索的规则。
应用程序标识	要搜索具有某个应用程序标识的攻击，您可以从**应用程序标识**列表框中选择此应用程序标识。

过程

1. 单击**攻击**选项卡。
2. 从**搜索**列表框中，选择**新建搜索**。
3. 选择下列其中一个选项:
   - 要装入先前已保存的搜索，请转至步骤 4。
   - 要创建新搜索，请转至步骤 7。
4. 使用下列其中一个选项选择先前已保存的搜索:
   - 从**可用的已保存搜索**列表中，选择要装入的已保存的搜索。
   - 在**输入已保存的搜索**或**从列表进行选择**字段中，输入要装入的搜索的名称。
5. 单击**装入**。
6. 可选。 在“编辑搜索”窗格中选中**设置为缺省值**复选框可以将此搜索设置为缺省搜索。如果将此搜索设置为缺省搜索，那么此搜索将在您每次访问**攻击**选项卡时自动执行并显示结果。
7. 在“时间范围”窗格中，选择要针对此搜索捕获的时间范围选项。 请参阅表 1。
8. 在“搜索参数”窗格中，定义特定搜索条件。 请参阅表 1。
9. 在“攻击源”窗格中，指定要搜索的攻击类型和攻击源:
   a. 从列表框中，选择要搜索的攻击类型。
   b. 输入搜索参数。 请参阅表 2。
10. 在“列定义”窗格中，定义要对结果执行的排序顺序:
    a. 从第一个列表框中，选择要作为搜索结果的排序依据的列。
    b. 从第二个列表框中，选择搜索结果的显示顺序。 选项包括“降序”和“升序”。
11. 单击**搜索**。

下一步做什么

在攻击选项卡上保存搜索条件

在“按源 IP”页面上搜索攻击

本主题提供有关如何在**攻击**选项卡的**按源 IP** 页面上搜索攻击的过程。

关于此任务

下表对可以用来在“按源 IP”页面上搜索攻击数据的搜索选项进行了描述:

表 44. “按源 IP”页面搜索选项

选项	描述
所有攻击	您可以选择此选项来搜索所有源 IP 地址，而与时间范围无关。
最近	您可以选择此选项，然后从此列表框中选择要搜索的时间范围。
特定的时间间隔	要指定要搜索的时间间隔，您可以选择“特定时间间隔”选项，然后选择下列其中一个选项: • **开始日期的范围** - 选中此复选框可以搜索与特定时间段内启动的攻击相关联的源 IP 地址。 选中此复选框后，请使用列表框来选择要搜索的日期。 • **最后一个事件/流范围** - 选中此复选框可以搜索与特定时间段内针对其发生最近已检测事件的攻击关联的源 IP 地址。选中此复选框后，请使用列表框来选择要搜索的日期。
搜索	“搜索”页面的多个窗格中提供了**搜索**图标。 如果您已完成配置搜索并希望查看结果，那么可以单击**搜索**。
源 IP	在此字段中，可以输入要搜索的源 IP 地址或 CIDR 范围。
规模	从此列表框中，可以指定规模，然后选择仅显示规模等于、小于或大于配置值的攻击。 范围是 0 - 10。
VA 风险	从此列表框中，可以指定 VA 风险，然后选择仅显示 VA 风险等于、小于或大于配置值的攻击。 范围是 0 - 10。
事件/流	在此列表框中，您可以指定事件或流计数，然后选择仅显示量级等于、小于或大于所配置值的攻击。
排除	您可以选中要从搜索结果中排除的攻击的复选框。 选项包括: • **处于活动状态的攻击** • **隐藏的攻击** • **关闭的攻击** • **处于非活动状态的攻击** • **受保护的攻击**

过程

1. 单击**攻击**选项卡。
2. 单击**按源 IP**。

3. 从**搜索**列表框中，选择**新建搜索**。
4. 在“时间范围”窗格中，选择要针对此搜索捕获的时间范围选项。 请参阅表 1。
5. 在“搜索参数”窗格中，定义特定搜索条件。 请参阅表 1。
6. 在“列定义”窗格中，定义要对结果执行的排序顺序:
   a. 从第一个列表框中，选择要作为搜索结果的排序依据的列。
   b. 从第二个列表框中，选择搜索结果的显示顺序。 选项包括**降序**和**升序**。
7. 单击**搜索**。

下一步做什么

在攻击选项卡上保存搜索条件

在“按目标 IP”页面上搜索攻击

在**攻击**选项卡的**按目标 IP** 页面上，可以搜索按目标 IP 地址分组的攻击。

关于此任务

下表对可以用来在“按目标 IP”页面上搜索攻击的搜索选项进行了描述:

表 45. “按目标 IP”页面搜索选项

选项	描述
所有攻击	您可以选择此选项来搜索所有目标 IP 地址，而与时间范围无关。
最近	您可以选择此选项，然后从此列表框中选择要搜索的时间范围。
特定时间间隔	要指定要搜索的特定时间间隔，您可以选择**特定时间间隔**选项，然后选择下列其中一个选项: • 要指定要搜索的特定时间间隔，您可以选择**特定时间间隔**选项，然后选择下列其中一个选项: • **最后一个事件/流范围** - 选中此复选框可以搜索与特定时间段内针对其发生最近已检测事件的攻击关联的目标 IP 地址。选中此复选框后，请使用列表框来选择要搜索的日期。
搜索	“搜索”页面的多个窗格中提供了**搜索**图标。 如果您已完成配置搜索并希望查看结果，那么可以单击**搜索**。
目标 IP	您可以输入要搜索的目标 IP 地址或 CIDR 范围。
规模	从此列表框中，可以指定规模，然后选择仅显示规模等于、小于或大于配置值的攻击。
VA 风险	从此列表框中，可以指定 VA 风险，然后选择仅显示 VA 风险等于、小于或大于配置值的攻击。 范围是 0 - 10。

表 45. “按目标 IP”页面搜索选项 (续)

选项	描述
事件/流	在此列表框中，您可以指定事件或流计数量级，然后选择仅显示事件或流计数等于、小于或大于所配置值的攻击。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**按目标 IP**。
3. 从**搜索**列表框中，选择**新建搜索**。
4. 在“时间范围”窗格中，选择要针对此搜索捕获的时间范围选项。 请参阅表 1。
5. 在“搜索参数”窗格中，定义特定搜索条件。 请参阅表 1。
6. 在“列定义”窗格中，定义要对结果执行的排序顺序:
   a. 从第一个列表框中，选择要作为搜索结果的排序依据的列。
   b. 从第二个列表框中，选择搜索结果的显示顺序。 选项包括**降序**和**升序**。
7. 单击**搜索**。

下一步做什么

在攻击选项卡上保存搜索条件

在“按网络”页面上搜索攻击

在**攻击**选项卡的**按网络**页面上，可以搜索按关联的网络分组的攻击。

关于此任务

下表对可以用来在“按网络”页面上搜索攻击数据的搜索选项进行了描述:

表 46. 用于在“按网络”页面上搜索攻击数据的搜索选项

选项	描述
网络	从此列表框中，可以选择要搜索的网络。
规模	从此列表框中，可以指定规模，然后选择仅显示规模等于、小于或大于配置值的攻击。
VA 风险	从此列表框中，可以指定 VA 风险，然后选择仅显示 VA 风险等于、小于或大于配置值的攻击。
事件/流	在此列表框中，您可以指定事件或流计数，然后选择仅显示事件或流计数等于、小于或大于所配置值的攻击。

过程

1. 单击**攻击**选项卡。
2. 单击**按网络**。
3. 从**搜索**列表框中，选择**新建搜索**。
4. 在“搜索参数”窗格中，定义特定搜索条件。 请参阅表 1。

5. 在“列定义”窗格中，定义要对结果执行的排序顺序:
   a. 从第一个列表框中，选择要作为搜索结果的排序依据的列。
   b. 从第二个列表框中，选择搜索结果的显示顺序。 选项包括**降序**和**升序**。
6. 单击**搜索**。

下一步做什么

在攻击选项卡上保存搜索条件

在攻击选项卡上保存搜索条件

在**攻击**选项卡上，可以保存配置的搜索条件，以便将来执行搜索时可以复用该条件。 保存的搜索条件不会到期。

过程

1. 过程
2. 执行搜索。 请参阅“攻击搜索”。
3. 单击**保存条件**。
4. 输入下列参数的值:

选项	描述
参数	描述
搜索名称	输入要分配给此搜索条件的名称。
管理组	单击**管理组**可管理搜索组。 请参阅管理搜索组。
时间范围选项:	选择下列其中一个选项: • **所有攻击** - 选择此选项将搜索所有攻击，而与时间范围无关。 • **最近** - 选择此选项，然后从此列表框中选择要搜索的时间范围。 • **特定时间间隔** - 要指定要搜索的特定时间间隔，请选择**特定时间间隔**选项，然后选择下列其中一个选项: 开始日期的范围 - 选中此复选框可以搜索在特定时间段内启动的攻击。 选中此复选框后，请使用列表框来选择要搜索的日期。最后一个事件/流范围 - 选中此复选框可以搜索特定时间段内针对其发生最近已检测事件的攻击。选中此复选框后，请使用列表框来选择您要搜索的日期。最后一个事件范围 - 选中此复选框可以搜索特定时间段内针对其发生最近已检测事件的攻击。选中此复选框后，请使用列表框来选择要搜索的日期。
设置为缺省值	选中此复选框可以将此搜索设置为缺省搜索。

5. 单击**确定**。

删除搜索条件

您可以删除搜索条件。

关于此任务

删除已保存的搜索后，与这个已保存搜索相关联的对象可能无法正常工作。 报告和异常检测规则就是使用了已保存的搜索条件的 QRadar 对象。 将保存的搜索删除后，请编辑相关联的对象，以确保其继续正常工作。

过程

1. 选择下列其中一个选项:
   - 单击**日志活动**选项卡。
   - 单击**网络活动**选项卡。
2. 从**搜索**列表框中，选择**新建搜索**或**编辑搜索**。
3. 在“已保存的搜索”窗格中，从**可用的已保存搜索**列表框中选择已保存的搜索。
4. 单击**删除**。
   - 如果已保存的搜索条件未与其他 QRadar 对象相关联，那么将显示确认窗口。
   - 如果已保存的搜索条件与其他对象相关联，那么将显示“删除已保存的搜索”窗口。此窗口列出了与所要删除的已保存搜索相关联的对象。 请记录相关联的对象。
5. 单击**确定**。
6. 选择下列其中一个选项:
   - 单击**确定**以继续。
   - 单击**取消**以关闭“删除已保存的搜索”窗口。

下一步做什么

如果已保存的搜索条件与其他 QRadar 对象相关联，请访问所记录的相关联对象，然后编辑这些对象，以除去或替换与删除的已保存搜索的关联。

使用子搜索优化搜索结果

使用子搜索可以在一组已完成的搜索结果中进行搜索。 子搜索用于优化搜索结果，而不必再次搜索数据库。

开始之前

定义要用作子搜索基础的搜索时，请确保禁用“实时（流式方法）”选项，并且不要对该搜索进行分组。

关于此任务

此功能不适用于分组搜索、进行中的搜索或者流方式下的搜索。

过程

1. 选择下列其中一个选项:
   - 单击**日志活动**选项卡。

- 单击**网络活动**选项卡。

2. 执行搜索。
3. 搜索完成后，请添加另一过滤器:
   a. 单击**添加过滤器**。
   b. 从第一个列表框中，选择要搜索的参数。
   c. 从第二个列表框中，选择要用于搜索的修饰符。 可用的修饰符列表取决于第一个列表中选择的属性。
   d. 在输入字段中，输入与此搜索相关的特定信息。
   e. 单击**添加过滤器**。

结果

“原始过滤器”窗格指定应用于基本搜索的原始过滤器。 “当前过滤器”窗格指定应用于子搜索的过滤器。 您可以清除子搜索过滤器，而不重新启动基本搜索。 请单击要清除的过滤器旁边的**清除过滤器**链接。 如果从“原始过滤器”窗格中清除了过滤器，那么将重新启动基本搜索。

删除已保存的子搜索条件的基本搜索条件后，仍可以访问已保存的子搜索条件。 如果添加过滤器，那么子搜索将在整个数据库中进行搜索，这是因为搜索功能不再以先前搜索的数据集作为搜索基础。

下一步做什么

保存搜索条件

管理搜索结果

您可以启动多个搜索，然后搜索在后台执行期间，您可以浏览到其他选项卡以执行其他任务。

可以对搜索进行配置，使搜索在完成时向您发送电子邮件通知。

在搜索执行期间的任意时刻，您可以返回到**日志活动**或**网络活动**选项卡，以查看部分或完整的搜索结果。

取消搜索

当搜索已排队或正在进行中时，您可以在“管理搜索结果”页面上取消搜索。

关于此任务

如果您在搜索正在进行时取消该搜索，那么将对取消操作之前累积的结果进行维护。

过程

1. 选择下列其中一个选项:
   - 单击**日志活动**选项卡。
   - 单击**网络活动**选项卡。
2. 从**搜索**菜单中，选择**管理搜索结果**。
3. 选择要取消的已排队或进行中的搜索结果。

4. 单击**取消**。
5. 单击**是**。

删除搜索

如果不再需要某个搜索结果，您可以从“管理搜索结果”页面中将其删除。

过程

1. 选择下列其中一个选项:
   - 单击**日志活动**选项卡。
   - 单击**网络活动**选项卡。
2. 从**搜索**菜单中，选择**管理搜索结果**。
3. 选择要删除的搜索结果。
4. 单击**删除**。
5. 单击**是**。

管理搜索组

通过使用“搜索组”窗口，您可以创建和管理事件、流和攻击搜索组。

借助这些组，您可以在**日志活动**、**网络活动**和**攻击**选项卡以及“报告”向导中轻松找到已保存的搜索条件。

查看搜索组

提供了一组缺省组和子组。

关于此任务

您可以查看“事件搜索组”、“流搜索组”或“攻击搜索组”窗口上的搜索组。

所有未分配到组的已保存的搜索位于**其他**组中。

“事件搜索组”、“流搜索组”和“攻击搜索组”窗口显示了各个组的下列参数。

表 47. “搜索组”窗口参数

参数	描述
名称	指定搜索组的名称。
用户	指定创建搜索组的用户名。
描述	指定搜索组的描述。
修改日期	指定搜索组的修改日期。

“事件搜索组”、“流搜索组”和“攻击搜索组”窗口工具栏提供了下列功能。

表 48. “搜索组”窗口工具栏功能

功能	描述
新建组	要创建新的搜索组，您可以单击**新建组**。 请参阅创建新的搜索组。

表 48. “搜索组”窗口工具栏功能 (续)

功能	描述
编辑	要编辑现有搜索组，您可以单击**编辑**。请参阅编辑搜索组。
复制	要将已保存的搜索复制到另一搜索组中，您可以单击**复制**。 请参阅将已保存的搜索复制到另一组中。
除去	要除去搜索组或者从搜索组中除去已保存的搜索，请选择要除去的项，然后单击**除去**。 请参阅除去组或者从组中除去已保存的搜索。

过程

1. 选择下列其中一个选项:
   - 单击**日志活动**选项卡。
   - 单击**网络活动**选项卡。
2. 选择**搜索 >编辑搜索**。
3. 单击**管理组**。
4. 查看搜索组。

创建新的搜索组

您可以创建新的搜索组。

过程

1. 选择下列其中一个选项:
   - 单击**日志活动**选项卡。
   - 单击**网络活动**选项卡。
2. 选择**搜索 编辑搜索**。
3. 单击**管理组**。
4. 选择要在其下创建新组的组的文件夹。
5. 单击**新建组**。
6. 在**名称**字段中，输入新组的唯一名称。
7. 可选。 在**描述**字段中，输入描述。
8. 单击**确定**。

编辑搜索组

您可以对搜索组的**名称**和**描述**字段进行编辑。

过程

1. 选择下列其中一个选项:
   - 单击**日志活动**选项卡。
   - 单击**网络活动**选项卡。
2. 选择**搜索 > 编辑搜索**。
3. 单击**管理组**。

4. 选择要编辑的组。
5. 单击**编辑**。
6. 编辑参数:
   - 在**名称**字段中输入新名称。
   - 在**描述**字段中输入新描述。
7. 单击**确定**。

将已保存的搜索复制到另一组中

您可以将已保存的搜索复制到一个或多个组中。

过程

1. 选择下列其中一个选项:
   - 单击**日志活动**选项卡。
   - 单击**网络活动**选项卡。
2. 选择**搜索 > 编辑搜索**。
3. 单击**管理组**。
4. 选择要复制的已保存的搜索。
5. 单击**复制**。
6. 在“项组”窗口上，选中要将已保存的搜索复制到的组的复选框。
7. 单击**分配组**。

除去组或者从组中除去已保存的搜索

您可以使用**除去**图标从组中除去搜索或除去搜索组。

关于此任务

从某个组中除去已保存的搜索时，已保存的搜索不会从系统中删除。 已保存的搜索将从该组中除去，并自动移动至**其他**组。

不能将下列组从系统中除去:

- 事件搜索组
- 流搜索组
- 攻击搜索组
- 其他

过程

1. 选择下列其中一个选项:
   - 单击**日志活动**选项卡。
   - 单击**网络活动**选项卡。
2. 选择**搜索 > 编辑搜索**。
3. 单击**管理组**。
4. 选择下列其中一个选项:
   - 选择要从组中除去的已保存的搜索。

- 选择要除去的组。

5. 单击**除去**。
6. 单击**确定**。

第 10 章 定制事件和流属性

通过使用事件和流的定制属性，可以对 QRadar 通常未规范化并显示的日志信息进行搜索、查看和报告。

可以从**日志活动**或**网络活动**选项卡上的多个位置创建事件和流的定制属性:

- 在**日志活动**选项卡中，双击一个事件，然后单击**抽取属性**。
- 在**网络活动**选项卡中，双击一个流，然后单击**抽取属性**。
- 您可以从“搜索”页面中创建或编辑事件或流的定制属性。从“搜索”页面创建定制属性时，不会从任何特定事件或流派生该属性；因此，不会预先填充“定制事件属性”窗口。您可以从其他来源复制并粘贴有效内容信息。

所需许可权

要创建定制属性，您需要有正确的许可权。

您必须具有“用户定义的事件属性”或“用户定义的流属性”许可权。

如果您具有管理许可权，那么还可以通过“管理”选项卡创建和修改定制属性。

单击**管理 > 数据源 > 定制事件属性** > 或**管理 > 数据源 > 定制流属性**。

请与管理员进行核对，以确保您具有正确的许可权。

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

定制属性类型

您可以创建定制属性类型。

创建定制属性时，可以选择创建正则表达式属性类型或计算的属性类型。

通过使用正则表达式 (Regex) 语句，可以从事件或流有效内容中抽取非规范化数据。

例如，您创建了一个报告，用于报告所有在 Oracle 服务器上进行了用户许可权更改的用户。报告了用户列表及这些用户更改另一帐户许可权的次数。但是，通常无法显示更改的实际用户帐户或许可权。您可以创建一个用于从日志中抽取此信息的定制属性，然后在搜索和报告中使用此属性。使用此功能要求您精通正则表达式 (Regex)。

正则表达式定义了要用作定制属性的字段。输入正则表达式语句后，可以根据有效内容对其进行验证。定义定制正则表达式模式时，请遵守 Java 编程语言所定义的正则表达式规则。

有关更多信息，您可以参阅 Web 上提供的正则表达式教程。一个定制属性可以与多个正则表达式关联。

解析事件或流时，将针对该事件或流测试各个正则表达式模式，直到某个正则表达式模式与有效内容匹配为止。第一个与事件或流有效内容匹配的正则表达式模式决定了要抽取的数据。

通过使用基于计算的定制属性，可以对现有的数字事件或流属性执行计算，以生成计算属性。

例如，通过用一个数字属性除以另一数字属性，可以创建显示百分比的属性。

创建基于正则表达式的定制属性

您可以创建基于正则表达式的定制属性，用于将事件或流有效内容与正则表达式匹配。

关于此任务

配置基于正则表达式的定制属性时，“定制事件属性”或“定制流属性”窗口将提供参数。下表提供了部分参数的参考信息。

表 49. “定制事件属性”窗口参数（正则表达式）

参数	描述
测试字段	
新属性	新属性名不能是规范化属性（例如，用户名、源 IP 或目标 IP）的名称。
针对规则、报告和搜索优化解析	在首次接收事件或流时解析并存储属性。选中此复选框后，该属性无需进一步解析即可用于报告、搜索或规则测试。 如果取消选中此复选框，那么每次应用报告、搜索或规则测试时，都会对该属性进行解析。
日志源	如果多个日志源与此事件相关联，那么此字段将显示“多个”一词以及日志源数。
正则表达式	这是用于从有效内容中抽取数据的正则表达式。 正则表达式区分大小写。 下列示例显示了样本正则表达式: • 电子邮件: `(.+@[^\.].*\.[a-z]{2,}$)` • URL: `(http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\S*)?$)` • 域名: `(http[s]?://(.+?)["/?:])` • 浮点数: `([-+]?\d*\.?\d*$)` • 整数: `([-+]?\d*$)` • IP 地址: `(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)` 捕获组必须括在圆括号内。
捕获组	捕获组将多个字符作为单一单元进行处理。 在捕获组中，字符通过一组圆括号进行分组。

表 49. “定制事件属性”窗口参数（正则表达式） (续)

参数	描述
已启用	如果取消选中此复选框，那么此定制属性不会显示在搜索过滤器或列的列表中，并且不会根据有效内容解析属性。

过程

1. 单击**日志活动**选项卡。
2. 如果您要以流方式查看事件或流，请单击**暂停**图标以暂停流。
3. 双击要用作定制属性基础的事件或流。
4. 双击要用作定制属性的基础的事件。
5. 单击**抽取属性**。
6. 在**属性类型选择**窗格中，选中**基于正则表达式**选项。
7. 配置定制属性参数。
8. 单击**测试**以根据有效内容测试正则表达式。
9. 单击**保存**。

结果

定制属性将作为一个选项显示在搜索页面上可用列的列表中。 要在事件或流列表中包含定制属性，您必须在创建搜索时从可用列的列表中选择定制属性。

相关概念:

第 134 页的『AQL 搜索字符串示例』
使用 Ariel Query Language (AQL) 可以从 Ariel 数据库中的事件、流以及 simarc 表中检索特定字段。

创建基于计算的定制属性

您可以创建一个基于计算的定制属性，用于将有效内容与正则表达式匹配。

关于此任务

配置基于计算的定制属性时，“定制事件属性”或“定制流属性”窗口提供以下参数:

表 50. “定制属性定义”窗口参数（计算）

参数	描述
属性定义	
属性名	输入此定制属性的唯一名称。 新属性名不能是规范化属性（例如用户名、源 IP 或目标 IP）的名称。
描述	输入此定制属性的描述。
属性计算定义	

表 50. “定制属性定义”窗口参数（计算） (续)

参数	描述
属性 1	从此列表框中，选择要在计算中使用的第一个属性。 选项包括所有数字规范化属性和数字定制属性。 您还可以指定特定的数字值。 从**属性 1** 列表框中，选中**用户定义**选项。这将显示**数字属性**参数。输入特定的数字值。
运算符	从此列表框中，选择要应用于计算中的所选属性的运算符。 选项包括: • 加 • 减 • 乘 • 除
属性 2	从此列表框中，选择要在计算中使用的第二个属性。 选项包括所有数字规范化属性和数字定制属性。 您还可以指定特定的数字值。 从**属性 1** 列表框中，选中**用户定义**选项。这将显示**数字属性**参数。输入特定的数字值。
已启用	选中此复选框可启用此定制属性。 如果取消选中该复选框，那么此定制属性不会显示在事件或流搜索过滤器或列的列表中，并且不会根据有效内容解析事件或流属性。

过程

1. 选择下列其中一项: 单击**日志活动**选项卡。
2. 可选。 如果您要以流方式查看事件或流，请单击**暂停**图标以暂停流。
3. 双击要用作定制属性基础的事件或流。
4. 单击**抽取属性**。
5. 在“属性类型选择”窗格中，选中**基于计算**选项。
6. 配置定制属性参数。
7. 单击**测试**以根据有效内容测试正则表达式。
8. 单击**保存**。

结果

定制属性现在将作为一个选项显示在搜索页面上可用列的列表中。 要在事件或流列表中包含定制属性，您必须在创建搜索时从可用列的列表中选择定制属性。

修改定制属性

您可以修改定制属性。

关于此任务

可以使用“定制事件属性”或“定制流属性”窗口来修改定制属性。

下表对定制属性进行了描述。

表 51. 定制属性窗口列

列	描述
属性名	指定此定制属性的唯一名称。
类型	指定此定制属性的类型。
属性描述	指定此定制属性的描述。
日志源类型	指定此定制属性所应用于的日志源类型的名称。 此列仅在“定制事件属性”窗口上显示。
日志源	指定此定制属性所应用于的日志源。 如果存在多个与此事件或流关联的日志源，那么此字段将显示“多个”一词以及日志源数。 此列仅在“定制事件属性”窗口上显示。
表达式	指定此定制属性的表达式。 此表达式视定制属性类型而定: 对于基于正则表达式的定制属性，此参数指定要用于从有效内容中抽取数据的正则表达式。 对于基于计算的定制属性，此参数指定要用于创建定制属性值的计算。
用户名	指定创建此定制属性的用户的名称。
已启用	指定是否已启用此定制属性。 此字段指定 true 或 false。
创建日期	指定此定制属性的创建日期。
修改日期	指定此定制属性的最近一次修改时间。

“定制事件属性”和和“定制流属性”工具栏提供了下列功能:

表 52. 定制属性工具栏选项

选项	描述
添加	单击**添加**可以添加新的定制属性。
编辑	单击**编辑**可以对所选定制属性进行编辑。
复制	单击**复制**可以复制所选定制属性。
删除	单击**删除**可以删除所选定制属性。

表 52. 定制属性工具栏选项 (续)

选项	描述
启用/禁用	单击**启用/禁用**可以启用或禁用所选列属性，以便在搜索过滤器或列的列表中进行解析和查看。

过程

1. 选择下列其中一项:
   - 单击**日志活动**选项卡。
   - 单击**网络活动**选项卡。
2. 从**搜索**列表框中，选择**编辑搜索**。
3. 单击**管理定制属性**。
4. 选择要编辑的定制属性，然后单击**编辑**。
5. 编辑所需参数。
6. 可选。 如果您编辑了正则表达式，请单击**测试**以根据有效内容测试正则表达式。
7. 单击**保存**。

复制定制属性

要根据现有定制属性创建新的定制属性，您可以复制现有定制属性，然后修改参数。

过程

1. 选择下列其中一项:
   - 单击**日志活动**选项卡。
   - 单击**网络活动**选项卡。
2. 从**搜索**列表框中，选择**编辑搜索**。
3. 单击**管理定制属性**。
4. 选择要复制的定制属性，然后单击**复制**。
5. 编辑所需参数。
6. 可选。 如果您编辑了正则表达式，请单击**测试**以根据有效内容测试正则表达式。
7. 单击**保存**。

删除定制属性

您可以删除定制属性，前提是该定制属性未与其他定制属性相关联。

过程

1. 选择下列其中一项:
   - 单击**日志活动**选项卡。
   - 单击**网络活动**选项卡。
2. 单击**日志活动**选项卡。
3. 从**搜索**列表框中，选择**编辑搜索**。
4. 单击**管理定制属性**。

5. 选择要删除的定制属性，然后单击**删除**。
6. 单击**是**。

第 11 章 规则管理

通过**日志活动**、**网络活动**和**攻击**选项卡，可以查看和维护规则。

本主题适用于具有**查看定制规则**或**维护定制规则**用户角色许可权的用户。

规则许可权注意事项

如果您具有“查看定制规则”和“维护定制规则”用户角色许可权，那么可以查看和管理您有权访问的网络区域的规则。

要创建异常检测规则，您必须对要在其中创建规则的选项卡具有相应的**维护定制规则**许可权。 例如，要能够在“日志活动”选项卡中创建异常检测规则，您必须具有**日志活动 > 维护定制规则**许可权。

有关用户角色许可权的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

规则概述

规则对事件、流或攻击执行测试，并且在满足所有测试条件时生成响应。

每条规则中的测试还可以引用其他构建块和规则。 您无需按任何特定顺序创建规则，这是因为每次添加、编辑或删除新规则时，系统都会检查依赖关系。 如果删除或禁用了由另一规则引用的规则，那么将显示警告，并且不会执行任何操作。

要获取缺省规则的完整列表，请参阅 *IBM Security QRadar SIEM Administration Guide*。

规则类别

规则分为两个类别，即定制规则和异常规则。

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。

异常检测规则对已保存的流或事件搜索的结果执行测试，作为检测网络中何时发生异常流量模式的一种方法。

异常检测规则对已保存的流或事件搜索的结果执行测试，作为检测网络中何时发生异常流量模式的一种方法。此规则类别包含下列规则类型：异常、阈值和行为。

异常规则对事件和流的流量进行测试以确定异常活动，例如存在新流量或未知流量（突然停止的流量，或者对象处于活动状态的时间长度存在百分比变化的流量）。 例如，您可以创建一条异常规则，用于将过去 5 分钟的平均流量与过去一小时的平均流量进行比较。 如果变化幅度超过 40%，那么此规则将生成响应。

阈值规则对事件和流的流量执行测试，以确定小于、等于或大于所配置阈值或者在指定范围内的活动。阈值可以基于所收集的任何数据。 例如，可以创建一条阈值规则，指定上午 8 点到下午 5 点之间不得有 220 个以上的客户机登录服务器。 第 221 个客户机尝试登录时，此阈值规则将生成警报。

行为规则对事件和流的流量进行测试，从而确定按有规律的季节性模式发生的行为的量变化。例如，如果邮件服务器在午夜通常每秒与 100 台主机进行通信，然后突然开始每秒与 1,000 台主机进行通信，那么行为规则将生成警报。

规则类型

有四种不同类型的规则；事件、流、公共和攻击。

事件规则

事件处理器以实时方式处理事件时，事件规则将对这些事件执行测试。您可以创建事件规则，用于检测单个事件（在某些属性内）或事件序列。 例如，如果要监视网络中不成功的登录尝试、访问多台主机或者随后进行渗透的侦察事件，那么可以创建事件规则。 事件规则创建攻击作为响应十分常见。

流规则

QFlow Collector 以实时方式处理流时，流规则将对这些流执行测试。 您可以创建流规则，用于检测单个流（在某些属性内）或流序列。 流规则创建攻击作为响应十分常见。

公共规则

公共规则用于对事件和流记录所共有的字段执行测试。例如，您可以创建公共规则以检测具有特定源 IP 地址的事件和流。公共规则创建攻击作为响应十分常见。

攻击规则

仅当对攻击进行了更改（例如，添加了新事件或者系统调度攻击以进行重估）时，攻击规则才会处理攻击。 攻击规则通过电子邮件发送通知作为响应十分常见。

规则条件

每条规则都可能包含函数、构建块或测试。

借助函数，您可以使用构建块和其他规则来创建多事件、多流或多攻击函数。可以使用支持布尔运算符（例如 OR 和 AND）的函数来连接规则。 例如，如果要连接事件规则，那么可以在事件与下列任意/全部规则函数匹配是使用。

构建块是不含响应的规则，用作多条规则中的公共变量，或者用于构建要在其他规则中使用的复杂规则或逻辑。 您可以将一组测试保存为构建块，以便与其他函数配合使用。 借助构建块，可以在其他规则中复用特定的规则测试。 例如，可以保存一个其中包含网络中所有邮件服务器的 IP 地址的构建块，然后使用该构建块从其他规则中排除这些邮件服务器。 提供了缺省构建块作为准则，您应该根据网络需求对这些构建块进行复查和编辑。

注: 缺省情况下，未装入构建块。 定义规则以便对构建块进行构建。

要获取构建块的完整列表，请参阅 *IBM Security QRadar SIEM Administration Guide*。

可以对事件、流或攻击的属性（例如源 IP 地址、事件严重性或事件率分析）运行测试。

规则响应

满足规则条件时，规则可以生成一个或多个响应。

规则可以生成下列其中一个或多个响应:

- 创建攻击。
- 发送电子邮件。
- 在“仪表板”功能部件上生成系统通知。
- 向引用集添加数据。
- 向引用数据集合添加数据。
- 对外部系统生成响应。
- 向可以在规则测试中使用的引用数据集合添加数据。
- 运行定制操作脚本以响应事件。

引用数据集合类型

必须先使用命令行界面 (CLI) 创建引用数据集合，然后才能将规则响应配置为向引用数据集合发送数据。 QRadar 支持下列数据集合类型:

引用集 这是一组派生自网络中发生的事件和流的元素，例如 IP 地址或用户名的列表。

引用映射
数据存储在记录中，后者将键映射到值。 例如，要关联网络中的用户活动，您可以创建一个使用 **Username** 参数作为键，且使用用户的 **Global ID** 作为值的引用映射。

集合的引用映射
数据存储在记录中，后者将键映射到多个值。 例如，要测试对某项专利授予的访问权，请使用 **Patent ID** 的定制事件属性作为键，并使用 **Username** 参数作为值。 使用集合映射来填充授权用户列表。

映射的引用映射
数据存储在记录中，该记录将一个键映射到另一个键，后一个键接着映射到单个值。 例如，要对网络带宽违例进行测试，您可以创建映射的映射。 使用 **Source IP** 参数作为第一个键，使用 **Application** 参数作为第二个键，并使用 **Total Bytes** 参数作为值。

引用表 在引用表中，数据存储在表中，这个表将一个键映射到另一个键，后一个键接着映射到单个值。 对于第二个键，指定了类型。 此映射类似于数据库表，该表中的每个列都与某种类型相关联。 例如，您可以创建一个引用表，这个表存储了 **Username** 参数作为第一个键，具有多个辅键（对于这些辅键，指定了用户定义的类型，例如 **IP 类型**），并使用 **Source IP** 或 **Source Port** 参数作为值。您可以配置规则响应，以添加此表中定义的一个或多个键。 另外，还可以向规则响应添加定制值。 定制值必须对辅键的类型有效。

注: 有关引用集和引用数据集合的信息，请参阅产品的《*管理指南*》。

查看规则

您可以查看规则的详细信息，包括测试、构建块和响应。

开始之前

根据用户角色许可权，您可以从**攻击**、**日志活动**或**网络活动**选项卡访问规则页面。

有关用户角色许可权的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

关于此任务

“规则”页面显示包含规则及其关联参数的列表。要查找您希望打开并查看其详细信息的规则，可以使用工具栏上的“组”列表框或**搜索规则**字段。

过程

1. 选择下列其中一个选项:
   - 单击**攻击**选项卡，然后在导航菜单上单击**规则**。
   - 单击**日志活动**选项卡，然后从工具栏上的**规则**列表框中选择**规则**。
   - 单击**网络活动**选项卡，然后从工具栏上的**规则**列表框中选择**规则**。
2. 从**显示**列表框中，选择**规则**。
3. 双击要查看的规则。
4. 查看规则详细信息。

结果

如果您具有**查看定制规则**许可权，但没有**维护定制规则**许可权，那么将显示**规则摘要**页面，并且规则不可编辑。 如果您具有**维护定制规则**许可权，那么将显示**规则测试堆栈编辑器**页面。 您可以查看并编辑规则详细信息。

创建规则

规则根据规则测试条件来评估传入的数据，以便从系统中生成响应。规则的条件符合时，可以执行多项操作。例如，您可配置系统对规则的响应，这包括生成攻击、发送电子邮件、启动扫描、添加参考数据或者提高或降低严重性之类的值。

开始之前

要创建新规则，您必须具有**攻击 > 维护定制规则**许可权。

关于此任务

定义规则测试时，请按处理搜索的方式处理规则，并尽可能针对最小的数据执行测试。以此方式执行测试有助于提高规则测试性能，并确保不会创建成本高昂的规则。为了优化性能，请以减少规则测试所评估数据的广义类别入手。例如，请以针对特定日志源类型、网络位置、流源或上下文的规则测试（R2L、L2R 和 L2L）入手。您执行的任何中等级别测试可能包括 IP 地址、端口流量或任何其他相关联的测试。请将有效内容测试和正则表达式测试用作最后的规则测试。

大部分规则测试评估单个条件，例如参考数据集合中是否存在某个元素，或者针对事件的属性来测试某个值。对于复杂比较，您可通过构建带有 WHERE 子句条件的 Ariel 查询语言 (AQL) 查询来测试事件规则。您可使用所有的 WHERE 子句函数来编写复杂

条件，这样就不需要运行许多单独的测试。例如，使用 AQL WHERE 子句来检查是否对参考集跟踪了入站 SSL 或 Web 流量。

过程

1. 在**攻击**、**日志活动**或**网络活动**选项卡中，单击**规则**。
2. 从**操作**列表中，选择规则类型。

   每种规则类型都以实时方式对来自不同来源的传入数据执行测试。例如，事件规则测试传入日志源数据，而攻击规则测试攻击参数以触发更多响应。
3. 在“规则测试堆栈编辑器”页面上的“规则”窗格中，在**应用**文本框中输入要对此规则指定的唯一名称。
4. 从列表框中，选择**本地**或**全局**。

   局部规则将事件和流发送到局部事件处理器以触发规则。这是缺省操作。

   全局规则将事件和流发送到中央事件处理器，这可能会降低控制台的性能。控制台上的定制规则引擎 (CRE) 跟踪事件匹配项，这些匹配项由部署中的每台受管主机提供。建立不完整匹配项或者需要更新计数器时，每台受管主机都向控制台上的 CRE 发送更新。当整条规则变为 true 时，控制台将触发规则响应。

   有关局部和全局规则测试的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
5. 从**测试组**列表中，选择一个或多个要添加到此规则的测试。CRE 将按顺序逐行评估规则测试。即，先评估第一项测试，此测试成功时，再评估下一行，直至达到最后一项测试为止。

   对于新的事件规则，如果选中**当事件与此 AQL 过滤器查询匹配时**测试，请在**输入 AQL 过滤器查询**文本框中输入 AQL WHERE 子句查询。

   了解有关针对未检测到的事件使用规则的更多信息:

   以下规则测试可单独触发，但是不会根据相同规则测试堆栈中的后续规则测试采取行动。

   - **当一种或多种日志源类型经过此时间（以秒计）仍无法检测到事件时**
   - **当一个或多个日志源经过此时间（以秒计）仍无法检测到事件时**
   - **当一个或多个日志源组经过此时间（以秒计）仍无法检测到事件时**

   传入事件不会激活这些规则测试，改为当在配置的特定时间间隔内未出现特定事件的情况下激活这些规则测试。QRadar 使用一个*观察程序任务*定期查询最近一次出现某一事件的时间（上次出现时间），并针对每个日志源存储该事件的这一时间。当上次出现时间与当前时间相距超出规则中配置的时间（以秒计）时触发此规则。
6. 要将配置的规则导出为构建块，以便与其他规则配合使用，请单击**导出为构建块**。

   构建块是没有任何响应的规则测试的子集。您可将构建块想像成可以在其他规则中使用的规则测试的可复用集合。一个常见的示例是，在“BB: 主机定义”构建块中填充服务器地址。然后，管理员可以按特定服务器类型（例如 VPN 服务器、邮件服务器或 LDAP 服务器）来排除或包括规则测试。
7. 在“规则响应”页面上，配置希望此规则生成的响应。

规则响应是所有规则测试均为 true 时，QRadar 设备执行的操作。规则变为 true 时，规则响应（例如电子邮件、系统日志消息和转发事件）在处理器上针对局部规则发生，并在控制台上针对全局规则发生。

相关概念:

第 176 页的『“规则响应”页面参数』

配置“规则响应”页面的参数，以指定您希望 IBM Security QRadar 如何在规则触发时做出响应。

创建异常检测规则

使用“异常检测规则”向导可创建一些规则，这些规则使用“日期和时间”测试来应用时间范围条件。

开始之前

要创建新的异常检测规则，您必须满足下列需求:

- 具有“维护定制规则”许可权。
- 执行分组搜索。

执行分组搜索并保存搜索条件后，将显示异常检测选项。

关于此任务

您必须具有相应的角色许可权才能创建异常检测规则。

要在**日志活动**选项卡上创建异常检测规则，您必须具有**日志活动维护定制规则**角色许可权。

要在**网络活动**选项卡上创建异常检测规则，您必须具有**网络维护定制规则**角色许可权。

异常检测规则使用该规则所基于的已保存搜索条件中的所有分组和过滤条件，但不使用搜索条件中的任何时间范围。

创建异常检测规则时，此规则将以缺省测试堆栈进行填充。 您可以编辑缺省测试，也可以向测试堆栈添加测试。 测试堆栈中必须至少包含一个“累积属性”测试。

缺省情况下，**单独地测试各个 [组] 的 [所选累积属性] 值**选项在“规则测试堆栈编辑器”页面上处于选中状态。

这将导致异常检测规则对每个事件组或流组的所选累积属性进行单独测试。例如，如果所选累积值为 **UniqueCount(sourceIP)**，那么此规则将对每个事件组或流组的每个唯一源 IP 地址进行测试。

单独地测试每个 [组] 的 [所选累积属性] 值选项是动态的。 **[所选累积属性]** 值取决于您为缺省测试堆栈的**此累积属性测试**字段选择的选项。 **[组]** 值取决于已保存的搜索条件中指定的分组选项。 如果提供了多个分组选项，那么文本可能会被截断。 将鼠标指针移动到文本上方可查看所有组。

过程

1. 单击**日志活动**或**网络活动**选项卡。
2. 执行搜索。
3. 从**规则**菜单中，选择要创建的规则类型。 选项包括:
   - 添加异常规则
   - 添加阈值规则
   - 添加行为规则
4. 阅读“规则”向导上的介绍性文本。 单击**下一步**。 已选中您先前选择的规则。
5. 单击**下一步**以查看“规则测试堆栈编辑器”页面。
6. 在**请在此处输入规则名称**字段中，输入要分配给此规则的唯一名称。
7. 要向规则添加测试，请完成下列步骤:
   a. 可选。 要对“测试组”列表框中的选项进行过滤，请在“请输入内容以进行过滤”字段中输入要过滤的文本。
   b. 从“测试组”列表框中，选择要添加到此规则的测试类型。
   c. 对于要添加到规则的每个测试，选中该测试旁边的 + 符号。
   d. 可选。 要将某个测试标识为已排除的测试，请在“规则”窗格中该测试的开头部分单击 and。 and 将显示为 and not。
   e. 单击带下划线的可配置参数，以定制测试的变量。
   f. 从对话框中，选择变量的值，然后单击**提交**。
8. 可选。 要测试每个事件或流组的总所选累积属性，请取消选中**分别测试每个 [组] 的 [所选累积属性] 值**复选框。
9. 在“组”窗格中，选中要将此规则分配到的组的复选框。 有关更多信息，请参阅规则组管理。
10. 在**备注**字段中，输入任何要针对此规则提供的备注。 单击**下一步**。
11. 在“规则响应”页面上，配置希望此规则生成的响应。 第 176 页的『“规则响应”页面参数』
12. 单击**下一步**。
13. 查看配置的规则。 单击**完成**。

规则管理任务

您可以对定制规则和异常规则进行管理。

可以根据需要启用和禁用规则。 另外，还可以编辑、复制或删除规则。

只能在**日志活动**和**网络活动**选项卡上创建异常检测规则。

要对缺省的以及先前创建的异常检测规则进行管理，必须使用**攻击**选项卡上的“规则”页面。

启用和禁用规则

调整系统时，您可以启用或禁用相应的规则，以确保系统生成对环境有意义的攻击。

关于此任务

您必须具有**攻击 > 维护定制规则**角色许可权才能启用或禁用规则。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 从**规则**页面上的**显示**列表框中，选择**规则**。
4. 选择要启用或禁用的规则。
5. 从**操作**列表框中，选择**启用/禁用**。

编辑规则

您可以编辑规则，以更改规则名称、规则类型、测试或响应。

关于此任务

您必须具有**攻击 > 维护定制规则**角色许可权才能启用或禁用规则。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 从**规则**页面上的**显示**列表框中，选择**规则**。
4. 双击要编辑的规则。
5. 从**操作**列表框中，选择**打开**。
6. 可选。 如果要更改规则类型，请单击**返回**并选择新的规则类型。
7. 在“规则测试堆栈编辑器”页面上，编辑参数。
8. 单击**下一步**。
9. 在“规则响应”页面上，编辑参数。
10. 单击**下一步**。
11. 查看编辑后的规则。 单击**完成**。

复制规则

您可以复制现有规则、输入规则的新名称，然后根据需要定制新规则中的参数。

关于此任务

您必须具有**攻击 > 维护定制规则**角色许可权才能启用或禁用规则。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 从**显示**列表框中，选择**规则**。
4. 选择要复制的规则。
5. 从**操作**列表框中，选择**复制**。
6. 在“为复制的规则输入名称”字段中，输入新规则的名称。 单击**确定**。

删除规则

您可以从系统中删除规则。

关于此任务

您必须具有**攻击 > 维护定制规则**角色许可权才能启用或禁用规则。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 从**显示**列表框中，选择**规则**。
4. 选择要删除的规则。
5. 从**操作**列表框中，选择**删除**。

规则组管理

如果您是管理员，那么能够创建、编辑和删除规则组。 通过将规则或构建块归类为组，可以有效地查看和跟踪规则。

例如，您可以查看所有与合规性相关的规则。

创建新规则时，可以将该规则分配到现有的组。 有关使用规则向导分配组的信息，请参阅创建定制规则或创建异常检测规则。

查看规则组

在“规则”页面上，您可以对规则或构建块进行过滤，以仅查看属于特定组的规则或构建块。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 从**显示**列表框中，选择您是希望查看规则还是构建块。
4. 从**过滤器**列表框中，选择要查看的组类别。

创建组

“规则”页面提供了缺省规则组，但您可以创建新组。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 单击**组**。
4. 从导航树中，选择要在其下方创建新组的组。
5. 单击**新建组**。
6. 输入下列参数的值:
   - **名称** - 请输入要分配给新组的唯一名称。 名称长度可达 255 个字符。

- **描述** - 请输入要分配给这个组的描述。 描述长度可达 255 个字符。

7. 单击**确定**。
8. 可选。 要更改新组的位置，请单击新组，并将文件夹拖动到导航树中的新位置。

将项分配给组

您可以将所选规则或构建块分配给组。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 选择要分配给组的规则或构建块。
4. 从**操作**列表框中，选择**分配组**。
5. 选择要将规则或构建块分配到的组。
6. 单击**分配组**。
7. 关闭**选择组**窗口。

编辑组

您可以编辑组以更改名称或描述。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 单击**组**。
4. 从导航树中，选择要编辑的组。
5. 单击**编辑**。
6. 更新下列参数的值:
   - **名称** - 请输入要分配给新组的唯一名称。 名称长度可达 255 个字符。
   - **描述** - 请输入要分配给这个组的描述。 描述长度可达 255 个字符。
7. 单击**确定**。
8. 可选。 要更改该组的位置，请单击新组，并将文件夹拖动到导航树中的新位置。

将项复制到另一组中

您可以将规则或构建块从一个组复制到其他组中。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 单击**组**。
4. 从导航树中，选择要复制到另一组中的规则或构建块。
5. 单击**复制**。
6. 选中要将规则或构建块复制到的组的复选框。
7. 单击**复制**。

从组中删除项

您可以从组中删除项。 从组中删除规则或构建块时，该项将仅从组中删除，并在“规则”页面上保持可用。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 单击**组**。
4. 使用导航树浏览到所要删除的项，并将其选中。
5. 单击**除去**。
6. 单击**确定**。

删除组

您可以删除组。 删除组后，该组的规则或构建块将仍显示在“规则”页面上。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 单击**组**。
4. 使用导航树浏览到所要删除的组，并将其选中。
5. 单击**除去**。
6. 单击**确定**。

编辑构建块

您可以对任何缺省构建块进行编辑，以满足部署需求。

关于此任务

构建块是可复用的规则测试堆栈，您可以将其作为组件包括在其他规则中。

例如，您可以编辑“BB:HostDefinition: 邮件服务器”构建块，以标识部署中的所有邮件服务器。 然后，可以将任何规则配置为从规则测试中排除这些邮件服务器。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 从**显示**列表框中，选择**构建块**。
4. 双击要编辑的构建块。
5. 如有必要，更新构建块。
6. 单击**下一步**。
7. 继续完成向导。 有关更多信息，请参阅创建定制规则。
8. 单击**完成**。

“规则”页面参数

对“规则”页面上的参数的描述。

已部署的规则的列表提供了每条规则的以下信息:

表 53. “规则”页面参数

参数	描述
规则名	显示规则名称。
组	显示此规则所分配到的组。有关组的更多信息，请参阅规则组管理。
规则类别	显示规则的规则类别。 选项包括“定制规则”和“异常检测规则”。
规则类型	显示规则类型。 规则类型包括: • 事件 • 流 • 公共 • 攻击 • 异常 • 阈值 • 行为 有关规则类型的更多信息，请参阅规则类型。
已启用	指示是已启用还是已禁用此规则。有关启用和禁用规则的更多信息，请参阅启用和禁用规则。
响应	显示规则响应（如果有）。 规则响应包括: • 分派新事件 • 电子邮件 • 日志通知 • SNMP • 引用集 • 引用数据 • IF-MAP 响应 有关规则响应的更多信息，请参阅规则响应。
事件/流计数	显示此规则导致产生攻击时，与此规则关联的事件或流的数目。
攻击计数	显示由此规则生成的攻击数。
来源	显示此规则是缺省规则（系统）还是定制规则（用户）。
创建日期	指定此规则的创建日期和时间。
修改日期	指定此规则的修改日期和时间。

“规则”页面工具栏

您可以使用“规则”页面工具栏来显示规则、构建块或组。 您可以管理规则组并处理规则。

“规则”页面工具栏提供了下列功能:

表 54. “规则”页面工具栏的功能

功能	描述
显示	在此列表框中，请选择是要在规则列表中显示规则还是构建块。
组	在此列表框中，请选择要在规则列表中显示的规则组。
组	单击**组**可以管理规则组。
操作	单击**操作**并选择下列其中一个选项: • **新建事件规则** - 选择此选项可以创建新的事件规则。 • **新建流规则** - 选择此选项可以创建新的流规则。 • **新建公共规则** - 选择此选项可以创建新的公共规则。 • **新建攻击规则** - 选择此选项可以创建新的攻击规则。 • **启用/禁用** - 选择此选项可以启用或禁用所选规则。 • **复制** - 选择此选项可以复制所选规则。 • **编辑** - 选择此选项可以编辑所选规则。 • **删除** - 选择此选项可以删除所选规则。 • **分配组** - 选择此选项可以将所选规则分配到规则组。
还原规则	单击**还原规则**可以将经过修改的系统规则还原为缺省值。 您单击**还原规则**时，将显示确认窗口。 还原规则时，将永久除去先前的所有修改。 要还原规则并维护修改后的版本，请复制此规则，并对修改后的规则使用**还原规则**选项。

表 54. “规则”页面工具栏的功能 (续)

功能	描述
搜索规则	请在**搜索规则**字段中输入搜索条件，然后单击**搜索规则**图标，或者按键盘上的 Enter 键。 所有满足搜索条件的规则都将显示在规则列表中。 将搜索下列参数以查找搜索条件的匹配项: • 规则名 • 规则（描述） • 备注 • 响应 “搜索规则”功能将尝试查找直接文本字符串匹配项。 如果找不到任何匹配项，那么“搜索规则”功能将尝试查找正则表达式 (regex) 匹配项。

“规则响应”页面参数

配置“规则响应”页面的参数，以指定您希望 IBM Security QRadar 如何在规则触发时做出响应。

注: 构建 AQL 查询时，如果将包含单引号的文本从任何文档复制粘贴到 IBM Security QRadar 中，那么将无法解析此查询。变通方法为可将此文本粘贴到 QRadar 中，并重新输入单引号，或者可以从 IBM Knowledge Center 复制粘贴此文本。

下表提供了“规则响应”页面参数。

表 55. 事件、流和公共规则响应页面参数

参数	描述
对事件添加注释	如果要对此事件添加注释，请选中此复选框，并输入要对此事件添加的注释。
丢弃检测到的事件	选中此复选框可以使正常情况下发送到 Magistrate 组件的事件强制发送到 Ariel 数据库，以用于报告或搜索。丢弃的事件将写入存储器，并绕过规则测试。 此事件不会显示在**攻击**选项卡中。
分派新事件	如果选中此复选框，那么除分派原始事件或流以外，那么还将分派新事件，并且新事件将像系统中的所有其他事件一样进行处理。 如果选中此复选框，那么除分派原始事件以外，还将分派新事件，并且新事件将像系统中的所有其他事件一样进行处理。 选中此复选框后，将显示**分派新事件**参数。 缺省情况下，此复选框处于未选中状态。
事件名称	请输入要在**攻击**选项卡中显示的事件唯一名称。

表 55. 事件、流和公共规则响应页面参数 (续)

参数	描述
事件描述	请输入事件描述。 此描述将显示在事件详细信息的“注释”窗格中。
严重性	在此列表框中，请选择事件严重性。 范围为 0（最低）到 10（最高），且缺省值为 0。严重性将显示在事件详细信息的“注释”窗格中。
可信性	在此列表框中，请选择事件可信性。 范围为 0（最低）到 10（最高），且缺省值为 10。 可信性将显示在事件详细信息的“注释”窗格中。
相关性	在此列表框中，请选择事件相关性。 范围为 0（最低）到 10（最高），且缺省值为 10。 相关性将显示在事件详细信息的“注释”窗格中。
高级别类别	在此列表框中，请选择处理事件时要让此规则使用的高级别事件类别。
低级别类别	在此列表框中，请选择处理事件时要让此规则使用的低级别事件类别。
对此攻击添加注释	要对此攻击添加注释，请选中此复选框并输入注释。
电子邮件	选中此复选框可以显示电子邮件选项。 **注**: 要更改**电子邮件语言环境**设置，请在**管理**选项卡上选择**系统设置**。
输入要通知的电子邮件地址	请输入此规则生成通知时要将其发送到的电子邮件地址。 使用逗号可以分隔多个电子邮件地址。
选择事件/流电子邮件模板	为此规则的关联电子邮件选择电子邮件模板。有关配置定制电子邮件通知的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
SNMP 陷阱	仅当在系统设置中配置了“SNMP 设置”参数时，才会显示此参数。 选中此复选框将使此规则能够发送 SNMP 通知（陷阱）。 SNMP 陷阱输出包含由 MIB 定义的系统时间、陷阱 OID 和通知数据。
发送到本地系统日志	如果要在本地记录事件或流，请选中此复选框。 缺省情况下，此复选框处于未选中状态。 **注**: 只有规范化事件才能以本地方式记录在设备上。 如果要发送原始事件数据，那么必须使用“发送到转发目标”选项将该数据发送到远程系统日志主机。
发送到转发目标	如果要在转发目标中记录事件或流，请选中此复选框。转发目标是供应商系统，例如 SIEM、凭单发放或报警系统。选中此复选框后，将显示转发目标列表。 针对要向其发送此事件或流的转发目标选中此复选框。 要添加、编辑或删除转发目标，请单击**管理目标**链接。

表 55. 事件、流和公共规则响应页面参数 (续)

参数	描述
通知	如果您希望作为此规则的结果生成的事件显示在“仪表板”选项卡的“系统通知”项中，请选中此复选框。 如果启用了通知，请配置**响应限制器**参数。
添加到引用集	如果您希望作为此规则的结果生成的事件向引用集添加数据，请选中此复选框。 要向引用集添加数据，请完成下列步骤: 1. 使用第一个列表框选择要添加的数据。选项包括所有规范化或定制数据。 2. 使用第二个列表框选择要将指定数据添加到的引用集。 **添加到引用集**规则响应提供了下列功能: **刷新** 单击**刷新**可以刷新第一个列表框，以确保列表最新。 **配置引用集** 单击**配置引用集**可以配置引用集。 仅当您具有管理许可权时，此选项才可用。
添加到引用数据	必须先使用命令行界面 (CLI) 创建引用数据集合，然后才能使用此规则响应。 有关如何创建和使用引用数据集合的更多信息，请参阅产品的《*管理指南*》。 如果您希望作为此规则的结果生成的事件添加到引用数据集合，请选中此复选框。 选中此复选框后，请选择下列其中一个选项: **添加到引用映射** 选择此选项可将数据发送到“单个键/多个值”对的集合。 您必须选择数据记录的键和值，然后选择要将数据记录添加到的引用映射。 **添加到集合的引用映射** 选择此选项可将数据发送到“键/单个值”对的集合。 您必须选择数据记录的键和值，然后选择要将数据记录添加到的集合引用映射。 **添加到映射的引用映射** 选择此选项可将数据发送到“多个键/单个值”对的集合。 必须依次选择第一个映射的键、第二个映射的键以及数据记录的值。 另外，还必须选择要将数据记录添加到的映射引用映射。 **添加到引用表** 选择此选项可将数据发送到“多个键/单个值”对的集合，在此集合中，对辅键指定了类型。 请选择要将数据添加到的引用表，然后选择主键。 为数据记录选择内部键（辅键）及其值。

表 55. 事件、流和公共规则响应页面参数 (续)

参数	描述
执行定制操作	您可以编写脚本以执行特定操作，从而响应网络事件。例如，您可以编写脚本以创建用于阻止网络中的特定源 IP 地址响应重复登录故障的防火墙规则。 选中此复选框，然后从**要执行的定制操作**列表中选择定制操作。 通过使用**管理**选项卡上的**定义操作**图标，您可以添加和配置定制操作。
在 IF-MAP 服务器上发布	如果在系统设置中配置并部署了 IF-MAP 参数，请选择此选项，以发布有关 IF-MAP 服务器的事件信息。
响应限制器	选中此复选框后，可以使用列表框来配置您期望此规则进行响应的频率。
启用规则	选中此复选框可以启用此规则。

下表提供了规则类型为“攻击”时的“规则响应”页面参数。

表 56. “攻击规则响应”页面参数

参数	描述
对检测到的攻击进行命名/添加注释	选中此复选框可以显示“名称”选项。
新攻击名称	请输入要对此攻击指定的名称。
攻击注释	请输入要在“攻击”选项卡中显示的攻击注释。
攻击名称	请选择下列其中一个选项: **此信息应该添加到攻击名称中** 如果您希望将事件名称信息添加到攻击名称中，请选择此选项。 **此信息应该设置或替换攻击名称** 如果您希望将配置的事件名称用作攻击名称，请选择此选项。
电子邮件	选中此复选框可以显示电子邮件选项。 **注:** 要更改**电子邮件语言环境**设置，请在**管理**选项卡上选择**系统设置**。
输入要通知的电子邮件地址	请输入此事件生成通知时要将其发送到的电子邮件地址。 使用逗号可以分隔多个电子邮件地址。
SNMP 陷阱	仅当在系统设置中配置了“SNMP 设置”参数时，才会显示此参数。 选中此复选框将使此规则能够发送 SNMP 通知（陷阱）。 对于攻击规则，SNMP 陷阱输出包含由 MIB 定义的系统时间、陷阱 OID 和通知数据。
发送到本地系统日志	如果要在本地记录事件或流，请选中此复选框。

表 56. “攻击规则响应”页面参数 (续)

参数	描述
发送到转发目标	如果要在转发目标中记录事件或流，请选中此复选框。转发目标是供应商系统，例如 SIEM、凭单发放或报警系统。选中此复选框后，将显示转发目标列表。 针对要向其发送此事件或流的转发目标选中此复选框。 要添加、编辑或删除转发目标，请单击**管理目标**链接。
在 IF-MAP 服务器上发布	如果在系统设置中配置并部署了 IF-MAP 参数，请选择此选项，以发布有关 IF-MAP 服务器的攻击信息。
响应限制器	选中此复选框后，可以使用列表框来配置您期望此规则进行响应的频率。
启用规则	选中此复选框可以启用此规则。 缺省情况下，此复选框处于选中状态。

下表提供了规则类型为“异常”时的“规则响应”页面参数。

表 57. “异常检测规则响应”页面参数

参数	描述
分派新事件	指定此规则除了分派原始事件或流之外，还将分派新事件，这些新事件将像系统中的所有其他事件一样进行处理。缺省情况下，此复选框处于选中状态并且无法取消选中。
事件名称	请输入要在“攻击”选项卡中显示的事件唯一名称。
事件描述	请输入事件描述。 此描述将显示在事件详细信息的“注释”窗格中。
攻击命名	请选择下列其中一个选项: **此信息应该添加到相关联攻击的名称中** 如果您希望将事件名称信息添加到攻击名称中，请选择此选项。 **此信息应该设置或替换相关联攻击的名称** 如果您希望将配置的事件名称用作攻击名称，请选择此选项。 **注**: 替换攻击名称之后，名称更改在关闭攻击之后才会生效。例如，如果某项攻击与多项规则相关联，并且最后一次事件未触发配置为覆盖攻击名称的规则，那么最后一次事件不会更新此攻击名称。攻击名称将改为保留覆盖规则所设置的名称。 **此信息不应添加到相关联攻击的名称中** 如果您不希望将事件名称信息添加到攻击名称中，请选中此选项。
严重性	范围为 0（最低）到 10（最高），且缺省值为 5。严重性将显示在事件详细信息的“注释”窗格中。
可信性	您可以使用列表框来选择事件的可信性。 范围为 0（最低）到 10（最高），且缺省值为 5。可信性将显示在事件详细信息的“注释”窗格中。

表 57. “异常检测规则响应”页面参数 (续)

参数	描述
相关性	您可以使用列表框来选择事件的相关性。 范围为 0（最低）到 10（最高），且缺省值为 5。相关性将显示在事件详细信息的“注释”窗格中。
高级别类别	在此列表框中，请选择处理事件时要让此规则使用的高级别事件类别。
低级别类别	在此列表框中，请选择处理事件时要让此规则使用的低级别事件类别。
对此攻击添加注释	要对此攻击添加注释，请选中此复选框并输入注释。
确保分派的事件是攻击的组成部分	作为此规则的结果，此事件将转发到 Magistrate 组件。 如果存在攻击，那么将添加此事件。如果“攻击”选项卡中未创建任何攻击，那么将创建新攻击。 显示的选项如下所示: **对攻击编制索引的依据** 指定新攻击基于事件名称。 缺省情况下，此参数处于启用状态。 **将“事件名称”从现在开始 X 秒内检测到的事件包括在攻击中** 选中此复选框，并输入您希望在**攻击**选项卡上包含源中已检测到的事件或流的秒数。
电子邮件	选中此复选框可以显示电子邮件选项。 **注:** 要更改**电子邮件语言环境**设置，请在**管理**选项卡上选择**系统设置**。
输入要通知的电子邮件地址	请输入此规则生成通知时要将其发送到的电子邮件地址。 使用逗号可以分隔多个电子邮件地址。
选择事件电子邮件模板	为此规则的关联电子邮件选择电子邮件模板。有关配置定制电子邮件通知的更多信息，请参阅 *IBM Security QRadar Administration Guide*。
通知	如果您希望作为此规则的结果生成的事件显示在**仪表板**选项卡的“系统通知”项中，请选中此复选框。 如果启用了通知，请配置**响应限制器**参数。
发送到本地系统日志	如果要在本地记录事件或流，请选中此复选框。缺省情况下，此复选框处于未选中状态。 **注:** 只有规范化事件才能以本地方式记录在 QRadar 设备上。如果要发送原始事件数据，那么必须使用“发送到转发目标”选项将该数据发送到远程系统日志主机。

表 57. “异常检测规则响应”页面参数 (续)

参数	描述
添加到引用集	如果您希望作为此规则的结果生成的事件向引用集添加数据，请选中此复选框。 要向引用集添加数据，请完成下列步骤: 1. 使用第一个列表框选择要添加的数据。选项包括所有规范化或定制数据。 2. 使用第二个列表框选择要将指定数据添加到的引用集。 **添加到引用集**规则响应提供了下列功能: **刷新** 单击**刷新**可以刷新第一个列表框，以确保列表最新。 **配置引用集** 单击**配置引用集**可以配置引用集。 仅当您具有管理许可权时，此选项才可用。
添加到引用数据	必须先使用命令行界面 (CLI) 创建引用数据集合，然后才能使用此规则响应。 有关如何创建和使用引用数据集合的更多信息，请参阅产品的《*管理指南*》。 如果您希望作为此规则的结果生成的事件添加到引用数据集合，请选中此复选框。 选中此复选框后，请选择下列其中一个选项: **添加到引用映射** 选择此选项可将数据发送到“单个键/多个值”对的集合。 您必须选择数据记录的键和值，然后选择要将数据记录添加到的引用映射。 **添加到集合的引用映射** 选择此选项可将数据发送到“键/单个值”对的集合。 您必须选择数据记录的键和值，然后选择要将数据记录添加到的集合引用映射。 **添加到映射的引用映射** 选择此选项可将数据发送到“多个键/单个值”对的集合。 必须依次选择第一个映射的键、第二个映射的键以及数据记录的值。 另外，还必须选择要将数据记录添加到的映射引用映射。 **添加到引用表** 选择此选项可将数据发送到“多个键/单个值”对的集合，在此集合中，对辅键指定了类型。 请选择要将数据添加到的引用表，然后选择主键。 为数据记录选择内部键（辅键）及其值。

表 57. “异常检测规则响应”页面参数 (续)

参数	描述
执行定制操作	您可以编写脚本以执行特定操作，从而响应网络事件。例如，您可以编写脚本以创建用于阻止网络中的特定源 IP 地址响应重复登录故障的防火墙规则。 选中此复选框，然后从**要执行的定制操作**列表中选择定制操作。 通过使用**管理**选项卡上的**定义操作**图标，您可以添加和配置定制操作。
在 IF-MAP 服务器上发布	如果在系统设置中配置并部署了 IF-MAP 参数，请选择此选项，以发布有关 IF-MAP 服务器的攻击信息。
响应限制器	选中此复选框后，可以使用列表框来配置您期望此规则进行响应的频率。
启用规则	选中此复选框可以启用此规则。 缺省情况下，此复选框处于选中状态。

SNMP 通知可能类似于:

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
 Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
 ICMP Destination Unreachable Communication with Destination Host is
 Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
 Offense description"
```

系统日志输出可能类似于:

```
Sep 28 12:39:01 localhost.localdomain ECS:
 Rule 'Name of Rule' Fired: 172.16.60.219:12642
 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
 1000398, Category: 1011, Notes: Event description
```

相关任务:

第 166 页的『创建规则』

规则根据规则测试条件来评估传入的数据，以便从系统中生成响应。规则的条件符合时，可以执行多项操作。例如，您可配置系统对规则的响应，这包括生成攻击、发送电子邮件、启动扫描、添加参考数据或者提高或降低严重性之类的值。

第 12 章 历史关联

使用历史关联可通过定制规则引擎 (CRE) 运行过去的事件和流，以标识已发生的威胁或安全事件。

限制: 您不能在 IBM Security QRadar Log Manager 中使用历史关联。有关 IBM Security QRadar SIEM 与 IBM Security QRadar Log Manager 之间的差异的更多信息，请参阅 第 5 页的『安全情报产品中的功能』。

缺省情况下，IBM Security QRadar SIEM 部署以接近实时的方式分析从日志源和流源收集的信息。 使用历史关联，您可以按开始时间或设备时间进行关联。*开始时间*是 QRadar 收到事件的时间。*设备时间*是在设备上发生事件的时间。

历史关联在以下情况中很有用:

分析批量数据

如果将数据成批装入到 QRadar 部署，那么可以使用历史关联根据实时收集的数据来关联数据。例如，要避免性能在正常营业时间下降，可以在每晚午夜从多个日志源装入事件。您可以使用关联数据按设备时间关联数据，以查看过去 24 小时内发生的网络事件序列。

测试新规则

您可以运行历史关联来测试新规则。例如，您的某个服务器最近遭到新的恶意软件的攻击，而您没有针对该恶意软件的就绪规则。您可以创建要针对该恶意软件测试的规则。因此，如果在攻击时设置了规则，您可以使用历史关联根据历史数据检查规则，以查看该规则是否会触发响应。同样地，您可以使用历史关联来确定攻击首次发生的时间或攻击的频率。您可以继续调整规则，然后将它移入生产环境。

重现已丢失或清除的攻击

如果您的系统因为停运或其他原因而丢失攻击，那么您可以通过对在那段时间进入的事件和流运行历史关联来重现攻击。

识别先前隐藏的威胁

了解有关最新安全威胁的信息后，您可以使用历史关联来识别已发生但尚未触发事件的网络事件。您可以快速测试已损害您所在组织的系统或数据的威胁。

历史关联概述

您可配置历史关联概要文件，以指定要分析的历史数据以及用于执行测试的规则集。触发规则时，将创建攻击。您可分配该攻击，以进行调查和补救。

数据选择

概要文件使用保存的搜索来收集要在运行中使用的历史事件和流数据。请确保您的安全概要文件授权查看要包括在历史关联运行中的事件和流。

规则选择和处理

QRadar 控制台仅根据历史关联概要文件中指定的规则来处理数据。

事件和流中同时存在的公共规则测试数据。您必须具有同时查看事件和流的许可权，然后才能将公共规则添加至概要文件。概要文件由无权同时查看事件和流的用户进行编辑时，将从此概要文件中自动除去公共规则。

您可以在历史关联概要文件中包含已禁用的规则。此概要文件运行时，已禁用的规则将根据传入事件和流进行评估。如果触发该规则，并且规则操作是生成攻击，那么将创建该攻击，即使该规则处于禁用状态也是如此。为了避免产生不必要的干扰，在历史关联期间将忽略规则响应，例如报告生成和邮件通知。

由于历史关联处理发生在单个位置，因此会将概要文件中包含的规则视为全局规则。处理不会将规则从本地更改为全局，但在历史关联运行期间对该规则的处理如同其是全局规则一样。某些规则（如有状态规则）可能不会与其在本地事件处理器上运行的常规关联中一样触发相同响应。例如，某个本地有状态规则用于跟踪同一用户名在 5 分钟内的五次失败登录，该规则的行为方式在常规关联和历史关联运行下不同。在常规关联下，该本地规则维护一个计数器，用于记录每个本地事件处理器收到的失败登录次数。在历史关联中，该规则针对整个 QRadar 系统维护单个计数器。在此情况下，相比于常规关联运行，可能会以不同方式创建攻击。

攻击创建

仅当触发规则并且规则操作指定必须创建攻击时，历史关联运行才会创建攻击。历史关联运行既不会添加到实时攻击中，也不会添加到在早期历史关联运行中创建的攻击，即使使用了同一概要文件也是如此。

历史关联运行可创建的最大攻击数为 100。在到达该限制时，历史关联运行将停止。

在复查实时攻击的同时，您可以在“威胁和安全性监视”仪表板和**攻击**选项卡上查看历史攻击。

创建历史关联概要文件

创建历史关联概要文件以通过定制规则引擎 (CRE) 重新运行过去的事件和流。此概要文件包含要在运行期间使用的数据集和规则的相关信息。

限制: 您只能在 IBM Security QRadar SIEM 中创建历史概要文件。不能在 IBM Security QRadar Log Manager 中创建历史概要文件。

开始之前

事件和流中同时存在的公共规则测试数据。您必须具有同时查看事件和流的许可权，然后才能将公共规则添加至概要文件。概要文件由无权同时查看事件和流的用户进行编辑时，将从此概要文件中自动除去公共规则。

关于此任务

您可以将概要文件配置为通过开始时间或设备时间进行关联。*开始时间*是事件到达事件收集器的时间。*设备时间*是在设备上发生事件的时间。事件可以在开始时间或设备时间进行关联。 流只能在开始时间进行关联。

您可以在概要文件中包括已禁用的规则。已禁用的规则在规则列表中以规则名称后的（**已禁用**）表示。

历史关联运行既不会添加到实时攻击中，也不会添加到在早期历史关联运行中创建的攻击，即使使用了同一概要文件也是如此。

过程

1. 打开“历史关联”对话框。
   - 在**日志活动**选项卡上，单击**操作 > 历史关联**。
   - 在**网络活动**选项卡上，单击**操作 > 历史关联**。
   - 在**攻击**选项卡上，单击**规则 > 操作 > 历史关联**。
2. 单击**添加**，然后选择**事件概要文件**或**流概要文件**。
3. 输入概要文件的名称并选择保存的搜索。 您只能使用非汇总的已保存搜索。
4. 在**规则**选项卡上，选择要对历史数据运行的规则，然后选择关联时间。

   如果您选中了**使用所有已启用的规则**复选框，那么您不能在概要文件中包括已禁用的规则。如果您要在概要文件中同时包括已启用和已禁用的规则，那么必须分别从规则列表中选择它们，然后单击**添加所选项**。
5. 在**调度**选项卡中，输入所保存搜索的时间范围，然后设定概要文件调度设置。
6. 在**摘要**选项卡上，复审配置并选择是否立即运行概要文件。
7. 单击**保存**。

   将概要文件放入队列中以等待处理。 基于调度的已排队概要文件优先于手动运行。

查看历史关联运行的相关信息

查看历史关联概要文件的历史记录，以查看有关该概要文件的过往运行情况的信息。您可以查看运行期间创建的攻击列表，以及与概要文件中已触发的规则匹配的事件或流的目录。您可以查看已加入队列、正在运行、已完成、已完成但发生错误以及已取消的历史关联运行的历史记录。

关于此任务

针对运行期间为每个唯一的源 IP 地址触发的每条记录，将创建历史关联目录，即使未创建攻击也是如此。此目录包含完全或部分匹配所触发规则的事件或流。

您不能从 QRadar 直接构建有关历史关联数据的报告。如果您要使用第三方程序来构建报告，那么您可以导出 QRadar 中的数据。

过程

1. 打开“历史关联”对话框。
   - 在**日志活动**选项卡上，单击**操作 > 历史关联**。
   - 在**网络活动**选项卡上，单击**操作 > 历史关联**。
   - 在**攻击**选项卡上，单击**规则 > 操作 > 历史关联**。
2. 选择某个概要文件，然后单击**查看历史记录**。
   a. 如果历史关联运行状态为**已完成**并且**攻击计数**为 0，那么概要文件规则未触发任何攻击。

b. 如果历史关联运行创建了攻击，那么请在**攻击计数**列中单击链接，以查看所创建的攻击的列表。 如果仅创建了一次攻击，那么将显示攻击摘要。

3. 在**目录**列中，单击链接以查看完全或部分匹配概要文件规则的事件的列表。

   事件列表中**开始时间**列表示 QRadar 接收事件的时间。

4. 单击**关闭**。

第 13 章 X-Force Threat Intelligence 订阅源集成

IBM Security X-Force Threat Intelligence 订阅源提供潜在恶意 IP 地址和 URL 的最新列表。此信息可以合并到规则、攻击和事件中，并可以在网络环境中任何不良活动威胁网络稳定性之前识别这些活动。

您必须具有 QRadar 许可证扩展才能将 X-Force Threat Intelligence 订阅源与 QRadar 配合使用。

对 X-Force Threat Intelligence 订阅源中的内容指定了威胁评分，您可以使用该评分来帮助划分通过此内容声声称的事件和攻击的优先级。来自这些情报源的数据将自动合并到 QRadar 关联和分析功能中，并以因特网威胁数据来增强其威胁检测功能。任何涉及这些地址的安全事件或网络活动数据将自动进行标记，从而将有价值的上下文添加到安全事故分析和调查中。

要对威胁划分优先级并识别需要更多检查安全事故，您可以选择要合并到 QRadar 规则、攻击和事件中的 X-Force 订阅源。 例如，您可以使用订阅源来识别以下类型的事故:

- 对动态 IP 地址范围的一系列登录尝试
- 与业务合作伙伴门户网站的匿名代理连接
- 内部端点与已知僵尸网络命令和控制之间的连接
- 端点与已知恶意软件分发站点之间的通信

X-Force Threat Intelligence 订阅源将对 IP 地址进行分类，然后对此分类指定置信度评级值。对于 IP 声誉数据的分类，将指定 0 到 100 的置信度因子值。此置信度值表示 X-Force 确信对来自此 IP 地址的数据进行了准确分类的程度。置信度因子值为 0 的垃圾邮件 IP 声誉分类表示源 IP 流量确定不是垃圾邮件，而值 100 表示确定的垃圾邮件源。当您微调规则时，可使用置信度因子值来调整规则触发器的敏感度。通过调整此置信度因子值，您可调整所生成的攻击数。

IP 地址将分为以下类别:

- 恶意软件主机
- 垃圾邮件源
- 动态 IP 地址
- 匿名代理
- 僵尸网络命令和控制
- 扫描 IP 地址

X-Force Threat Intelligence 订阅源还会对 URL 地址进行分类。 例如，URL 地址可能会分类为约会、赌博或色情站点。 要查看 URL 分类的完整类别列表，请访问 IBM X-Force Exchange Web 站点 (https://exchange.xforce.ibmcloud.com/faq)。

您必须先创建定制事件属性以便从有效内容中抽取 URL，然后才能使用基于 URL 的规则。 已经为来自多个源（例如，Blue Coat SG 和 Juniper Networks Secure Access）的事件定义了 URL 定制属性。

有关创建定制事件属性的更多信息，请参阅定制事件和流属性。

X-Force Threat Intelligence 更新和服务器

将 IBM Security X-Force Threat Intelligence 订阅源添加到 QRadar 中之后，您可以立即接受高级威胁数据。

总体而言，来自 X-Force 的数据集每 3 分钟更新一次，并且 QRadar Console 负责处理所有的外部通信。

对于 X-Force 数据更新、许可、仪表板窗口小部件订阅源和 QRadar 自动更新，都会联系下列服务器:

表 58. X-Force 服务器

联系的服务器	服务器描述
www.iss.net	QRadar 的 X-Force Threat Intelligence 仪表板窗口小部件 (AlertCon/RSS 订阅源)
update.xforce-security.com	IP 声誉和 URL 数据的 X-Force Threat Intelligence 订阅源更新服务器
license.xforce-security.com	X-Force Threat Intelligence 许可服务器
qmmunity.q1labs.com	QRadar 自动更新。有关自动更新服务器的更多信息，请参阅 www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21958881)。

在 IBM Security QRadar 中启用 X-Force 规则

通过将 X-Force IP 声誉情报订阅源许可证添加至 QRadar 系统，可添加增强型 X-Force 规则。

过程

1. 单击**日志活动**选项卡。
2. 在工具栏上，单击**规则 > 规则**。
3. 从**组**菜单中，单击 **XForce Premium**。

   组列可能会同时显示旧款规则和增强型规则。缺省情况下，X-Force 旧款规则处于禁用状态。但是，您可能会看到处于启用状态的旧款规则。请使用较新的增强型规则，而不要使用利用远程网络的旧款规则。已除去远程网络选项。
4. 通过选中规则行并单击**操作 > 启用/禁用**，禁用任何旧款规则和 X-Force Premium 规则。

增强的 X-Force Threat Intelligence 规则

将 X-Force Threat Intelligence 订阅源添加到 QRadar 之后，您可以开始使用增强 X-Force 规则组中的规则。

以下规则包含在**增强型 X-Force 规则**组内。 可以按原样使用它们，也可以对它们进行定制。

以下规则基于 IP:

X-Force Premium: 与可能的恶意软件主机的内部连接
此通信指示很可能进行了感染客户机系统或下载了恶意软件的尝试。

X-Force Premium: 与匿名代理进行通信的内部主机
*匿名代理*是已知用于掩饰身份的地址。 它们通常由恶意软件使用或在高级持续威胁期间用于隐藏与外部源的通信的源。 这些地址可能与恶意软件通信或数据外泄之类的活动相关。

X-Force Premium: 内部邮件服务器向可能的垃圾邮件主机发送邮件
通常，与垃圾邮件主机进行通信的邮件服务器将被用于不正当用途。

X-Force Premium: 与已知垃圾邮件发送主机进行通信的非邮件服务器
此行为强有力地指示服务器已受到损害并且将被用作垃圾邮件中继设备。

X-Force Premium: 与外部动态 IP 进行通信的非服务器
动态分配的 IP 地址通常与因特网上的合法服务器不相关。 与动态地址进行通信的内部工作站可能表示存在可疑的内部活动或者恶意软件或僵尸网络活动。

X-Force Premium: 服务器启动的与动态主机的连接
通常，服务器与具有固定身份而非动态 IP 地址的主机进行通信。

由于 URL 是已传输数据的更具体的指示符，因此基于 URL 的规则比基于 IP 的规则更准确。

以下规则基于 URL:

X-Force Premium: 与僵尸网络命令和控制 URL 进行通信的内部主机
合法服务器有时可能会被用于在特定的 URL 地址提供僵尸网络连接。

X-Force Premium: 与恶意软件 URL 的内部主机通信
合法服务器有时可能会被用于在特定 URL 地址提供恶意软件。

创建使用 URL 分类来监视对特定类型 Web 站点的访问的规则

您可以创建用于在内部网络的用户访问分类为“赌博 Web 站点”的 URL 地址时发送电子邮件通知的规则。

开始之前

要使用 URL 分类规则，您必须预订 X-Force Threat Intelligence 订阅源。

要创建新规则，您必须具有**攻击 > 维护定制规则**许可权。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**规则**。
3. 从**操作**列表中，选择**新建事件规则**。
4. 阅读“规则”向导上的介绍性文本，然后单击**下一步**。
5. 单击**事件**，然后单击**下一步**。
6. 从**测试组**列表框中，选择 **X-Force 测试**。
7. 单击**当 X-Force 将此 URL 属性分类为下列其中一种类别时**测试旁边的加号 (+)。

8. 在“规则”窗格的**请在此处输入规则名称**字段中，输入要分配给此规则的唯一名称。
9. 从列表框中，选择**本地**或**全局**。
10. 单击带下划线的可配置参数，以定制测试的变量。
    a. 单击 **URL（定制）**。
    b. 选择包含从有效内容中抽取的 URL 的 URL 属性，然后单击**提交**。
    c. 单击**下列其中一中类别**。
    d. 从 X-Force URL 类别中选择**赌博/彩票**，单击**添加 +** 并单击**提交**。
11. 要将配置的规则作为构建块导出，以便与其他规则配合使用，请完成下列步骤:
    a. 单击**导出为构建块**。
    b. 输入此构建块的唯一名称。
    c. 单击**保存**。
12. 在“组”窗格中，选中要将此规则分配到的组的复选框。
13. 在**备注**字段中，输入要针对此规则提供的备注，然后单击**下一步**。
14. 在“规则响应”页面上，单击**电子邮件**，然后输入接收通知的电子邮件地址。 有关事件规则的其他响应参数的信息，请参阅事件、流和公共规则响应页面参数。
15. 单击**下一步**。
16. 如果规则准确，请单击**完成**。

在 X-Force Exchange 中查找 IP 地址和 URL 信息

使用 IBM Security QRadar 中的右键单击菜单选项来查找在 IBM Security X-Force Exchange 上找到的有关 IP 地址和 URL 的信息。您可以使用 QRadar 搜索、攻击和规则中的信息来进一步搜索或将有关 IP 地址和 URL 的信息添加到 X-Force Exchange 集合。

关于此任务

搜索安全性问题时，您可以添加公共或专用信息来跟踪集合中的数据。

*集合*是用于存储调查期间找到的信息的存储库。 可以使用集合来保存 X-Force Exchange 报告、注释或任何其他内容。 X-Force Exchange 报告同时包含保存该报告时的报告版本，以及指向报告的当前版本的链接。 集合还包含具有 wifi 样式记事本的段（时间线），可以在其中添加与集合相关的注释。

有关 X-Force Exchange 的更多信息，请参阅 X-Force Exchange (https://exchange.xforce.ibmcloud.com/)。

过程

1. 要从 QRadar 查找 X-Force Exchange 中的 IP 地址，请遵循以下步骤:
    a. 选择**日志活动**或**网络活动**选项卡。
    b. 右键单击要在 X-Force Exchange 中查看的 IP 地址，然后选择**更多选项 > 插件选项 > X-Force Exchange 查找**来打开 X-Force Exchange 界面。
2. 要从 QRadar 查找 X-Force Exchange 中的 URL，请遵循以下步骤:
    a. 选择**攻击**选项卡或**攻击**选项卡上提供的事件详细信息窗口。

b. 右键单击要在 X-Force Exchange 中查找的 URL，然后选择**插件选项 > X-Force Exchange 查找**来打开 X-Force Exchange 界面。

管理误报

您可使用 X-Force Threat Intelligence 来管理规则触发器的敏感度，以减少网络中的误报数。使用误报调整功能可以防止事件和流关联到攻击。

置信度因子

X-Force 将对 IP 声誉数据进行分类，并对该分类指定 0 到 100 的置信度因子值，其中 0 表示不信任，而 100 表示确信。例如，X-Force 可能会将某个源 IP 地址分类为扫描 IP，并指定置信度因子为 75，这是中高度级别的置信度。

如何输入置信度值?

请在 QRadar 中的以下 X-Force 规则测试中输入置信度值: **当 X-Force 将此主机属性分类为此类别且置信度值等于此数量时**

有关设置置信度值的准则

置信度因子是其中一个可用来帮助限制触发的规则所创建的攻击数的主要工具。根据您所需的保护级别，您可将置信度值调整为与您的网络环境最为匹配的级别。

在 DMZ 中，您可能希望选择较高的置信度值，例如，95% 或更高的值，因为您不需要调查此区域中的许多攻击。使用此级别的置信度时，IP 地址很有可能与列示的类别匹配。如果有 95% 的程度确信某台主机提供恶意软件，那么您需要了解该主机。

对于更为安全的网络区域，例如服务器池，您可降低置信度值。通过降低置信度级别，有可能识别更多威胁，并且您需要进行的调查工作较少，因为威胁与特定的网段相关。

为了进行最优的误报调整，请按分段来管理规则触发器。请查看网络基础结构，并确定哪些资产需要较高级别的保护，而哪些资产不需要。您可以为不同的网段应用不同的置信度值。使用构建块可以对常用的测试进行分组，以便可以在规则中使用这些测试。

基于 URL 的规则

您可能会看到来自共享虚拟托管站点的误报，这是因为一个站点可能提供合法内容，而同一 IP 地址的另一站点可能提供恶意软件。在共享虚拟托管设置中，URL 信息比较有帮助，这是因为 URL 是所传输数据的更具体指示符。基于 URL 的规则可能比基于 IP 的规则更为准确。

对于基于 URL 的规则，您必须创建定制事件属性以便从有效内容中抽取 URL。

有关调整误报的更多信息，请参阅 *Tuning Guide*。

第 14 章 报告管理

您可以使用**报告**选项卡来创建、编辑、分发和管理报告。

详尽、灵活的报告选项符合您的各种法规标准，例如 PCI 合规性。

您可以创建自己的定制报告，也可以使用缺省报告。可以定制缺省报告并变更其名称，然后将它们分发给其他用户。

如果系统包含大量报告，那么刷新**报告**选项卡可能需要很长时间。

注: 如果您运行的是 Microsoft Exchange Server 5.5，那么不可用的字体字符可能会显示在通过电子邮件发送的报告的主题行中。 要解决此问题，请下载并安装 Microsoft Exchange Server 5.5 的 Service Pack 4。 有关更多信息，请与 Microsoft 支持人员联系。

时区注意事项

要确保报告功能使用正确的日期和时间来报告数据，您的会话必须与您所在时区同步。

在 QRadar 产品安装和设置期间已配置时区。 请与管理员进行核对，以确保您的 QRadar 会话与您所在时区同步。

报告选项卡许可权

管理用户可以查看其他用户创建的所有报告。

非管理用户只能查看自己创建的报告，或者查看其他用户共享的报告。

报告选项卡参数

报告选项卡显示缺省报告和定制报告的列表。

通过**报告**选项卡，您可以查看有关报告模板的统计信息，对报告模板执行操作，查看生成的报告以及删除生成的内容。

如果报告未指定时间间隔调度，那么您必须手动生成报告。

您可以将鼠标悬停在任何报告上，以便在工具提示中预览报告摘要。 摘要指定报告配置和报告所生成的内容类型。

报告布局

报告可以包含一些数据元素，并且可以采用各种样式表示网络和安全数据，例如表、折线图、饼图和条形图。

选择报告布局时，请考虑要创建的报告的类型。 例如，对于显示多个对象的图形内容，请勿选择小图表容器。 每个图形都包含图注以及从中派生内容的网络列表；请选择足够大的容器来存放数据。 要预览各个图表显示数据的方式，请参阅图形类型。

图表类型

创建报告时，必须为要包含在报告中的各个图表选择图表类型。

图表类型确定了生成的报告显示数据和网络对象的方式。 可以对具有多项特征的数据制图，并在生成的单个报告中创建图表。

您可以使用下列任何图表类型:

- **无** - 使用此选项将在报告中显示一个空容器。 在报告中创建空白空间时，此选项可能非常有用。 如果对任何容器选择**无**选项，那么该容器不需要任何进一步配置。
- **资产漏洞** - 使用此图表可查看部署中各个已定义资产的漏洞数据。您可以在 VA 扫描检测到漏洞时生成“资产漏洞”图表。 此图表在安装 IBM Security QRadar Vulnerability Manager 后可用。
- **连接** - 仅当您购买了 IBM Security QRadar Risk Manager 并获得此产品的使用授权后，才会显示此图表选项。有关更多信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。
- **设备规则** - 仅当您购买了 IBM Security QRadar Risk Manager 并获得此产品的使用授权后，才会显示此图表选项。有关更多信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。
- **设备未使用的对象** - 仅当您购买了 IBM Security QRadar Risk Manager 并获得此产品的使用授权后，才会显示此图表选项。有关更多信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。
- **事件/日志** - 使用此图表可查看事件信息。 您可以使图表以**日志活动**选项卡中已保存的搜索中的数据为基础。可以定制要在生成的报告中显示的数据。 可以将图表配置为对可配置的时间段内的数据进行绘制。 此功能将帮助您检测事件趋势。 有关已保存的搜索的更多信息，请参阅数据搜索。
- **日志源** - 使用此图表来导出或报告日志源。 选择要显示在报告中的日志源和日志源组。按报告列对日志源进行排序。 包括在已定义的时间段内未报告的日志源。 包括在指定时间内创建的日志源。
- **流** - 使用此图表可查看流信息。 您可以使图表以“网络活动”选项卡中已保存的搜索中的数据为基础。 这将使您能够定制要在生成的报告中显示的数据。 您可以使用已保存的搜索将图表配置为对可配置的时间段内的流数据进行绘制。 此功能将帮助您检测流趋势。 有关已保存的搜索的更多信息，请参阅数据搜索。
- **排名靠前的目标 IP** - 使用此图表可显示所选网络位置中排名靠前的目标 IP。
- **排名靠前的攻击** - 使用此图表可显示所选网络位置目前发生的排名靠前的攻击。
- **排名靠前的源 IP** - 使用此图表可显示攻击您的网络或业务资产的排名靠前的攻击源（IP 地址），并对这些攻击源进行排序。
- **漏洞** - 仅当您购买了 IBM Security QRadar Vulnerability Manager 并获得此产品的使用授权后，才会显示“漏洞”选项。 有关更多信息，请参阅 *IBM Security QRadar Vulnerability Manager User Guide*。

“报告”选项卡工具栏

使用此工具栏可以对报告执行一些操作。

下表确定了“报告”工具栏选项并对这些选项进行了描述。

表 59. “报告”工具栏选项

选项	描述
组	
管理组	单击**管理组**可管理报告组。 通过使用“管理组”功能部件，可以将报告组织为功能组。 您可以与其他用户共享报告组。
操作	单击**操作**可以执行下列操作: • **创建** - 选中此选项可创建新的报告。 • **编辑** - 选中此选项可对所选报告进行编辑。 您也可以双击报告来编辑内容。 • **复制** - 选中此选项可复制或重命名所选报告。 • **分配组** - 选中此选项可将所选报告分配给报告组。 • **共享** - 选中此选项可与其他用户共享所选报告。 您必须具有管理特权才能共享报告。 • **切换调度** - 选中此选项可将所选报告切换为活动或非活动状态。 • **运行报告** - 选中此选项可生成所选报告。 要生成多个报告，请按住 Control 键并单击要生成的报告。 • **对原始数据运行报告** - 选中此选项可使用原始数据生成所选报告。 当您希望在所需累计数据可用之前生成报告时，此选项非常有用。 例如，如果要在自创建报告后的整整一周经过之前运行每周报告，那么可以使用此选项生成报告。 • **删除报告** - 选择此选项可以删除所选报告。 要删除多个报告，请按住 Control 键并单击要删除的报告。 • **删除生成的内容** - 选中此选项可删除针对所选行生成的所有内容。 要删除生成的报告，请按住 Control 键并单击要删除的生成的报告。
隐藏交互式报告	选中此复选框可隐藏不活动报告模板。 **报告**选项卡将自动刷新，并且仅显示活动报告。 取消选中此复选框将显示处于隐藏状态的不活动报告。

表 59. “报告”工具栏选项 (续)

选项	描述
搜索报告	在**搜索报告**字段中输入搜索条件，然后单击**搜索报告**图标。将对下列参数运行搜索，以确定哪些参数满足指定的条件: • 报告标题 • 报告描述 • 报告组 • 报告组 • 报告作者用户名

图形类型

每种图表类型都支持多种可用于显示数据的图形类型。

网络配置文件决定了图表描绘网络流量时使用的颜色。每个 IP 地址都使用唯一的颜色进行描绘。下表提供了有关图表中如何使用网络数据和安全数据的示例。该表描述了可用于每种图形的图表类型。

表 60. 图形类型

图形类型	可用的图表类型
折线图	• 事件/日志 • 流 • 连接 • 漏洞
堆积折线图	• 事件/日志 • 流 • 连接 • 漏洞
条形图	• 事件/日志 • 流 • 资产漏洞连接 • 连接 • 漏洞
水平条形图	• 排名靠前的源 IP • 排名靠前的攻击 • 排名靠前的目标 IP
堆积条形图	• 事件/日志 • 流 • 连接

表 60. 图形类型 (续)

图形类型	可用的图表类型
饼图	• 事件/日志 • 流 • 资产漏洞 • 连接 • 漏洞
表	• 事件/日志 • 流 • 排名靠前的源 IP • 排名靠前的攻击 • 排名靠前的目标 IP • 连接 • 漏洞 要在表中显示内容，您必须设计具有完整页面宽度容器的报告。
聚集表	可用于“资产漏洞”图表。 要在表中显示内容，您必须设计具有完整页面宽度容器的报告。

下列图形类型可用于 QRadar Log Manager 报告:

- 折线图
- 堆积折线图
- 条形图
- 堆积条形图
- 饼图
- 表图

注: 创建条形图和堆积条形图报告时，图注以固定格式显示，大部分情况下其中条形或条形部分以按颜色编码的标签来表示。如果选择时间作为 x 轴的值，那么可以在 x 轴上创建时间间隔。

创建定制报告

使用“报告”向导可创建和定制新报告。

开始之前

您必须具有相应的网络许可权才能与其他用户共享生成的报告。

有关许可权的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

关于此任务

“报告”向导提供了有关如何设计、调度和生成报告的逐步指导。

此向导使用下列关键元素来帮助您创建报告:

- **布局** - 各个容器的位置和大小
- **容器** - 特色内容的占位符
- **内容** - 容器中放置的图表的定义

创建每周或每月生成的报告后，必须经过预定时间，生成的报告才能返回结果。 对于调度的报告，必须等待调度的时间段后才能构建结果。 例如，每周搜索需要 7 天才能完成构建数据。 此搜索将在 7 天后返回结果。

指定报告的输出格式时，请考虑所生成报告的文件大小可以是 1 到 2 兆字节，具体取决于所选输出格式。 PDF 格式大小较小，并且不会使用大量磁盘存储空间。

过程

1. 单击**报告**选项卡。
2. 从**操作**列表框中，选择**创建**。
3. 在“欢迎使用“报告”向导！”窗口中，单击**下一步**。
4. 请选择下列其中一个选项:

选项	描述
手动方式	缺省情况下，报告只生成 1 次。 您可以根据需要多次生成报告。
每小时	将报告调度为在每小时结束时生成一次。 使用前一小时中的数据。 从列表框中，选择报告周期的开始和结束时间范围。 在此时间范围内，将每小时生成一次报告。 时间以半小时为增量提供。 对于**开始时间**和**结束时间**字段，缺省值都为凌晨 1:00。
每周	将报告调度为使用上周的数据每周生成一次。 选择要在星期几生成报告。 缺省值为星期一。 在此列表框中，请选择报告周期的开始时间。 时间以半小时为增量提供。 缺省值为凌晨 1:00。
每月	将报告调度为使用上月的数据每月生成一次。 在此列表框中，请选择要生成报告的日期。 缺省值为每月的第一天。 选择报告周期的开始时间。 时间以半小时为增量提供。 缺省值为凌晨 1:00。

5. 在**允许手动生成此报告**窗格中，单击**是**或**否**。
6. 配置报告的布局:
   a. 从**方向**列表框中，为页面方向选择**纵向**或**横向**。
   b. 从“报告”向导中显示的 6 个布局选项中选择其中一项。
   c. 单击**下一步**。
7. 为下列参数指定值:

参数	值
报告标题	标题长度可达 100 个字符。 请勿使用特殊字符。
徽标	在此列表框中，选择徽标。
标记页数选项	在此列表框中，选择在报告上显示页数的位置。 您可以选择不显示页数。
报告分类	输入此报告的分类。 您可以输入的最大长度为 75 个字符。 您可以使用前导空格、特殊字符和双字节字符。 报告分类显示在报告的页眉和页脚。 您可能希望将报告分类为机密、高度机密、敏感或内部。

8. 配置报告中的各个容器:
   a. 从**图表类型**列表框中，选择图表类型。
   b. 在“容器详细信息”窗口上，配置图表参数。

      注: 您还可以创建资产的已保存搜索。 从**要使用的搜索**列表框中，选择已保存的搜索。
   c. 单击**保存容器详细信息**。
   d. 如果选择多个容器，请重复步骤 a 到 c。
   e. 单击**下一步**。
9. 预览“布局预览”页面，然后单击**下一步**。
10. 选中要生成的报告格式的复选框，然后单击**下一步**。

    要点: 可扩展标记语言仅可用于表。
11. 选择报告的分发通道，然后单击**下一步**。 选项包括下列分发通道:

选项	描述
报告控制台	选中此复选框可将生成的报告发送到**报告**选项卡。 **报告控制台**是缺省分发通道。
选择应该能够查看生成的报告的用户。	选中**报告控制台**复选框后，将显示此选项。 从用户列表中，选择要授权其查看所生成报告的用户。
选择所有用户	仅当您选中**报告控制台**复选框后，才会显示此选项。 如果要授权所有用户查看所生成报告，请选中此复选框。 您必须具有相应的网络许可权才能与其他用户共享生成的报告。
电子邮件	如果要使用电子邮件来分发所生成的报告，请选中此复选框。

选项	描述
输入报告分发电子邮件地址	仅当您选中**电子邮件**复选框后，才会显示此选项。 请输入每个要接收所生成报告的收件人的电子邮件地址；使用逗号分隔电子邮件地址列表。此参数的最大字符数为 255。 电子邮件收件人将从 no_reply_reports@qradar 接收此电子邮件。
包括作为附件的报告（仅限于非 HTML）	仅当您选中**电子邮件**复选框后，才会显示此选项。 选中此复选框可以将生成的报告作为附件发送。
包括指向“报告控制台”的链接	仅当您选中**电子邮件**复选框后，才会显示此选项。 选中此复选框将在电子邮件中包括指向“报告控制台”的链接。

12. 在“完成”页面上，输入下列参数的值。

选项	描述
报告描述	输入此报告的描述。 此描述将显示在“报告摘要”页面以及生成的报告分发电子邮件中。
请选择希望此报告属于其成员的任何组	选择要将此报告分配到的组。有关组的更多信息，请参阅报告组。
是否要立即运行报告?	如果要在向导完成时生成报告，请选中此复选框。 缺省情况下，此复选框处于选中状态。

13. 单击**下一步**以查看报告摘要。
14. 在“报告摘要”页面上，选择摘要报告上提供的选项卡以预览报告配置。

结果

这将立即生成报告。 如果您在向导的最后一页上取消选中了**是否要立即运行报告**复选框，那么此报告将进行保存，并在安排的时间生成。 报告标题就是生成的报告的缺省标题。如果您重新配置报告以输入新的报告标题，那么此报告将另存为具有新名称的新报告；但是，原始报告将保持不变。

编辑报告

通过使用“报告”向导，可以对任何缺省报告或定制报告进行编辑以进行更改。

关于此任务

您可以使用或定制大量缺省报告。 缺省的**报告**选项卡显示了报告列表。 每个报告都捕获并显示现有数据。

注: 定制要手动生成的调度报告时，请选择时间范围**结束日期**，然后再选择**开始日期**。

过程

1. 单击**报告**选项卡。
2. 双击要定制的报告。
3. 在“报告”向导中，更改参数以定制报告，使其生成所需内容。

结果

如果您重新配置报告以输入新的报告标题，那么此报告将另存为具有新名称的新报告；但是，原始报告将保持不变。

查看生成的报告

在**报告**选项卡上，如果报告已经生成了内容，那么**格式**列中将显示一个图标。 您可以单击此图标来查看报告。

关于此任务

报告生成内容后，**生成的报告**列将显示一个列表框。 此列表框显示所有生成的内容，这些内容按报告的时间戳记进行组织。 最新报告将显示在列表顶部。如果报告没有生成任何内容，那么**生成的报告**列中将显示**无**值。

表示所生成报告的报告格式的图标将显示在**格式**列中。

可以 PDF、HTML、RTF、XML 和 XLS 格式生成报告。

注: XML 和 XLS 格式仅可用于那些使用单一图表表格格式（纵向或横向）的报告。

您只能查看管理员授权您访问的报告。 管理用户可以访问所有报告。

如果您使用 Mozilla Firefox Web 浏览器并且选择了 RTF 报告格式，那么 Mozilla Firefox Web 浏览器将启动一个新的浏览器窗口。 启动这个新窗口是 Mozilla Firefox Web 浏览器配置所致，并且不会影响 QRadar。 您可以关闭此窗口并继续 QRadar 会话。

过程

1. 单击**报告**选项卡。
2. 从**生成的报告**列的列表框中，选择要查看的报告的时间戳记。
3. 单击要查看的格式的图标。

删除生成的内容

删除生成的内容时，将删除所有根据报告模板生成的报告，但保留报告模板。

过程

1. 单击**报告**选项卡。
2. 选择要将生成的内容删除的报告。
3. 从**操作**列表框中，单击**删除生成的内容**。

手动生成报告

可以将报告配置为自动生成，但是，您随时可以手动生成报告。

关于此任务

生成报告时，“下一次运行时间”列将显示下列三条消息中的一条:

- **正在生成** - 正在生成此报告。
- **已排队（位于队列中）** - 此报告已排队以等待生成。 此消息指示了此报告在队列中的位置。 例如，第 1 个（共 3 个）。
- **（x 小时 x 分钟 y 秒）** - 已安排运行此报告。 此消息是倒数计时器，用于指定下次运行此报告的时间。

您可以选择**刷新**图标来刷新视图，包括**下一次运行时间**列中的信息。

过程

1. 单击**报告**选项卡。
2. 选择要生成的报告。
3. 单击**运行报告**。

下一步做什么

生成报告后，可以在“已生成的报告”列中查看生成的报告。

复制报告

要创建与现有报告非常类似的报告，您可以复制要建模的报告，然后对其进行定制。

过程

1. 单击**报告**选项卡。
2. 选择要复制的报告。
3. 从**操作**列表框中，单击**复制**。
4. 为这个报告输入新名称（不含空格）。

下一步做什么

您可以对复制的报告进行定制。

共享报告

您可以与其他用户共享报告。 共享报告时，您需要向另一用户提供所选报告的副本，以便于编辑或调度。

关于此任务

用户对共享报告进行的任何更新不会影响该报告的原始版本。

您必须具有管理特权才能共享报告。 另外，管理用户必须与新用户共享所有必需报告后，新用户才能查看和访问报告。

您只能与那些具有相应访问权限的用户共享报告。

过程

1. 单击**报告**选项卡。
2. 选择要共享的报告。
3. 从**操作**列表框中，单击**共享**。
4. 从用户列表中，选择要与之共享此报告的用户。

标记报告

要标记报告，可以导入徽标和特定图像。要使用定制徽标来标记报告，必须先上载并配置徽标，然后再开始使用“报告”向导。

开始之前

确保要使用的图形的大小为 144 x 50 像素，且背景为白色。

要确保浏览器显示新徽标，请将浏览器高速缓存清空。

关于此任务

在支持多个徽标时，报告标记对于您的企业十分有益。 上载图像时，该图像将自动保存为可移植网络图形 (PNG)。

上载新图像并将其设置为缺省图像时，新的缺省图像不会应用于先前生成的报告。 对先前生成的报告更新徽标要求您根据该报告手动生成新内容。

如果上载长度超出报告头支持能力的图像，那么该图像将自动调整大小以适合报告头；此大小的高度约为 50 像素。

过程

1. 单击**报告**选项卡。
2. 在导航菜单中，单击**标记**。
3. 单击**浏览**以浏览系统中的文件。
4. 选择要上载的徽标所在的文件。 单击**打开**。
5. 单击**上载图像**。
6. 选择要用作缺省徽标的徽标，然后单击**设置缺省图像**。

报告组

您可以将报告归类为各个功能组。 如果您将报告归类为组，那么可以高效地对报告进行组织和查找报告。

例如，您可以查看所有与支付卡行业数据安全标准 (PCIDSS) 合规性相关的报告。

缺省情况下，**报告**选项卡显示所有报告的列表，但您可以将报告分类为组，例如:

- 合规性
- 执行
- 日志源

- 网络管理
- 安全性
- VoIP
- 其他

创建新报告时，可以将报告分配到现有组，也可以创建新组。 您必须具有管理访问权才能创建、编辑或删除组。

有关用户角色的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

创建报告组

您可以创建新的组。

过程

1. 单击**报告**选项卡。
2. 单击**管理组**。
3. 使用导航树选择要在其下创建新组的组。
4. 单击**新建组**。
5. 输入下列参数的值:
   - **名称** - 输入新组的名称。名称长度可达 255 个字符。
   - **描述** - 可选。 输入此组的描述。 描述长度可达 255 个字符。
6. 单击**确定**。
7. 要更改新组的位置，请单击新组，并将文件夹拖动到导航树中的新位置。
8. 关闭“报告组”窗口。

编辑组

您可以编辑报告组以更改名称或描述。

过程

1. 单击**报告**选项卡。
2. 单击**管理组**。
3. 从导航树中，选择要编辑的组。
4. 单击**编辑**。
5. 如有必要，更新参数的值:
   - **名称** - 输入新组的名称。名称长度可达 255 个字符。
   - **描述** - 可选。 输入此组的描述。 描述长度可达 255 个字符。此字段是可选的。
6. 单击**确定**。
7. 关闭“报告组”窗口。

共享报告组

您可以与其他用户共享报告组。

开始之前

您必须具有管理许可权才能与其他用户共享报告组。

有关许可权的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

您不能使用内容管理工具 (CMT) 来共享报告组。

有关 CMT 的更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*

关于此任务

在“报告组”窗口上，共享用户可以查看报告列表中的报告组。

用户对共享报告组进行的任何更新不会影响该报告的原始版本。 只有所有者才能删除或修改。

用户复制或运行共享报告时，创建报告的副本。 用户可以编辑或调度已复制的报告组中的报告。

组共享选项覆盖为该组中的报告配置的先前报告共享选项。

过程

1. 单击**报告**选项卡。
2. 在**报告**窗口上，单击**管理组**。
3. 在**报告组**窗口上，选择要共享的报告组并单击**共享**。
4. 在**共享选项**窗口上，选择下列其中一个选项。

选项	描述
缺省（从父代继承）	未共享报告组。 任何已复制的报告组或生成的报告都保留在用户报告列表中。 为该组中的每个报告都分配了任何已配置的父报告共享选项。
与所有人共享	与所有用户共享报告组。
与符合以下条件的用户共享...	与特定用户共享报告组。 **用户角色** 从用户角色列表中选择并按添加图标 (+)。 **安全概要文件** 从安全概要文件列表中选择并按添加图标 (+)。

5. 单击**保存**。

结果

在“报告组”窗口上，共享用户可以查看报告列表中的报告组。 生成的报告显示基于安全概要文件设置的内容。

将报告分配给组

您可以使用**分配组**选项将报告分配给另一组。

过程

1. 单击**报告**选项卡。
2. 选择要分配给组的报告。
3. 从**操作**列表框中，选择**分配组**。
4. 从**项组**列表中，选中要将此报告分配到的组的复选框。
5. 单击**分配组**。

将报告复制到另一组中

使用**复制**图标可将报告复制到一个或多个报告组中。

过程

1. 单击**报告**选项卡。
2. 单击**管理组**。
3. 从导航树中，选择要复制的报告。
4. 单击**复制**。
5. 选择要将报告复制到的组。
6. 单击**分配组**。
7. 关闭“报告组”窗口。

除去报告

使用**除去**图标可以从组中除去报告。

关于此任务

从组中除去报告后，该报告将仍然在**报告**选项卡中存在。 该报告不会从系统中除去。

过程

1. 单击**报告**选项卡。
2. 单击**管理组**。
3. 从导航树中，浏览到要除去的报告所在的文件夹。
4. 从组列表中，选择要除去的报告。
5. 单击**除去**。
6. 单击**确定**。
7. 关闭“报告组”窗口。

声明

此信息为在美国提供的产品和服务而开发。

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

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区:

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。 某些国家或地区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 Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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。

此处包含的任何性能数据都是在受控环境中测得的。 因此，在其他操作环境中获得的数据可能会有明显的不同。 有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。 此外，有些测量是通过推算而估计的， 实际结果可能会有差异。 本文档的用户应当验证其特定环境的适用数据。

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来源中获取。 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。

所有关于 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。

显示的所有 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，如果与实际商业企业使用的名称和地址有任何相似之处，纯属巧合。

如果您正在查看本信息的软拷贝，图片和彩色图例可能无法显示。

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。当前的 IBM 商标列表，可从 Web 站点 www.ibm.com/legal/copytrade.shtml 上“版权和商标信息”部分获取。

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。

UNIX 是 The Open Group 在美国和其他国家或地区的注册商标。

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。

其他公司、产品和服务名称可能是其他公司的商标或服务标记。

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）。

有关使用各种技术（包括 cookie）来达到这些目的的更多信息，请参阅 IBM 隐私策略 (http://www.ibm.com/privacy) 和 IBM 在线隐私声明 (http://www.ibm.com/privacy/details) 中标题为“Cookies, Web Beacons and Other Technologies”的部分，以及“IBM Software Products and Software-as-a-Service Privacy Statement”(http://www.ibm.com/software/info/product-privacy)。

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 214 页的『(F)』 第 214 页的『(G)』 第 214 页的『(H)』 第 214 页的『(J)』 第 215 页的『(K)』 第 215 页的『(L)』 第 215 页的『(M)』 第 215 页的『(P)』 第 215 页的『(Q)』 第 215 页的『(R)』 第 216 页的『(S)』 第 216 页的『(T)』 第 216 页的『(W)』 第 216 页的『(X)』 第 216 页的『(Y)』 第 217 页的『(Z)』 第 217 页的『A』 第 217 页的『C』 第 218 页的『D』 第 218 页的『F』 第 218 页的『H』 第 218 页的『I』 第 218 页的『L』 第 218 页的『M』 第 218 页的『N』 第 218 页的『O』 第 218 页的『Q』 第 218 页的『R』 第 219 页的『S』 第 219 页的『T』 第 219 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

[H]

[J]

[K]

[L]

[M]

[P]

[Q]

[R]

[S]

[T]

[W]

[X]

[Y]

[Z]

C

I

P

Q

R

X

[特别字符]

Printed in China