IBMSecurity QRadar Risk Manager

V 7.2.4

入门指南

IBM

备注

使用此信息及其支持的产品前，请阅读第 27 页的『声明』中的信息。

产品信息

本文档适用于 IBM QRadar Security Intelligence Platform V7.2.4 及后续发行版，直到被本文档的更新版本所取代。

目录

IBM Security QRadar Risk Manager 简介

本信息用于 IBM® Security QRadar® Risk Manager。 QRadar Risk Manager 是一款设施，用于监视设备配置、模拟网络环境的更改，以及为网络中的风险和脆弱性划分优先级。

目标受众

本指南的目标受众是负责在您的网络中安装和配置 QRadar Risk Manager 系统的网络管理员。

技术文档

要在 Web 上查找 IBM Security QRadar 产品文档，包括所有翻译文档，请访问 IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome)。

有关如何在 QRadar 产品库中访问更多技术文档的信息，请参阅访问 IBM Security 文档技术说明 (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)。

与客户支持人员联系

有关与客户支持人员联系的信息，请参阅支持和下载技术说明 (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:

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

第 1 章 IBM Security QRadar Risk Manager 入门

IBM Security QRadar Risk Manager 是一款单独安装的设施。 使用 QRadar Risk Manager 可监视设备配置、模拟网络环境的更改，以及为网络中的风险和漏洞划分优先级。

QRadar Risk Manager 可从 IBM Security QRadar SIEM 控制台上的**风险**选项卡访问。

通过向管理员提供工具来完成以下任务，QRadar Risk Manager 增强了 QRadar SIEM:

- 集中风险管理。
- 使用拓扑来查看网络。
- 配置和监视网络设备。
- 查看网络设备之间的连接。
- 搜索防火墙规则。
- 查看现有规则以及已触发规则的事件计数。
- 搜索网络设备的设备和路径。
- 监视和审计网络以确保合规性。
- 在网络上定义、安排和运行开发模拟。
- 搜索脆弱性。

集中风险管理与提高的信息智能合规性可能涉及许多内部团队的协作。作为带有附加风险管理设施的下一代 SIEM，与第一代 SIEM 产品相比，我们减少了所需的步骤数。我们为在 QRadar SIEM 中进行管理的资产提供了网络拓扑和风险评估。

评估过程中，您可以通过聚集与关联，将系统、安全性、风险分析与网络信息统一起来，从而能够完整地了解网络环境。 还可定义环境的门户，这一门户具有的可视性与效率是使用手动过程和其他点产品技术无法实现的。

第 2 章 部署 IBM Security QRadar Risk Manager

您的 QRadar Risk Manager 设施安装了最新版本的 QRadar Risk Manager 软件。

必须安装 IBM SecurityQRadar Risk Manager 评估设施。 该软件需要激活，您必须为 QRadar Risk Manager 设施分配一个 IP 地址。

如果您激活软件和分配 IP 地址时需要协助，请联系客户支持。

本设施已准备好从您的网络设备接受信息。

有关使用 IBM Security QRadar Risk Manager 的信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。

要在您的环境中部署 QRadar Risk Manager，您必须:

1. 确保安装了最新版本的 IBM Security QRadar SIEM。
2. 确保满足所有安装前需求。
3. 设置并打开 QRadar Risk Manager 设施。
4. 将 QRadar Risk Manager 插件安装到 QRadar SIEM 控制台上。
5. 在 QRadar SIEM 和 QRadar Risk Manager 设施之间建立通信。
6. 为 QRadar Risk Manager 用户定义用户角色。

安装之前

在安装 IBM Security QRadar Risk Manager 之前，必须完成 IBM Security QRadar SIEM 控制台的安装过程。 最佳做法是，将 QRadar SIEM 与 QRadar Risk Manager 安装在同一台网络交换机上。

必须复查以下信息:

- 配置防火墙端口访问
- 确定网络设置
- QRadarRisk Manager 中不受支持的功能
- 受支持的 Web 浏览器

在安装 IBM Security QRadar Risk Manager 评估设施之前，请确保:

- 有足够的空间容纳两单元设施
- 安装了机架导轨和架子

另外，您可能需要 USB 键盘和标准 VGA 监视器来访问 QRadar SIEM 控制台。

配置防火墙上的端口访问

IBM Security QRadar Console 与 IBM Security QRadar Risk Manager 之间的防火墙必须允许某些端口上的流量。

确保位于 QRadar SIEM 控制台与 QRadar Risk Manager 之间的任何防火墙都允许以下端口上的流量:

- 端口 443 (HTTPS)
- 端口 22 (SSH)
- 端口 37 UDP（时间）

识别网络设置

在开始安装流程之前，必须收集关于网络设置的信息。

收集以下关于网络设置的信息:

- 主机名
- IP 地址
- 网络掩码地址
- 子网掩码
- 缺省网关地址
- 主域名系统 (DNS) 服务器地址
- 辅助 DNS 服务器（可选）地址
- 使用网络地址转换 (NAT) 电子邮件服务器名称的公共 IP 地址
- 电子邮件服务器名称
- 网络时间协议 (NTP) 服务器（仅对控制台）或时间服务器名称

QRadar Risk Manager 中不受支持的功能

知晓哪些功能不受 IBM Security QRadar Risk Manager 的支持，这很重要。

以下功能在 QRadar Risk Manager 中不受支持:

- 高可用性 (HA)
- 边界网关协议 (BGP) 的动态路由选择、开放式最短路径优先协议 (OSPF) 或 路由信息协议 (RIP)
- IPv6
- 非连续的网络掩码
- 负载均衡的路由
- 参考映射
- 存储转发

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 1. QRadar 产品支持的 Web 浏览器

Web 浏览器	支持的版本
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
32 位 Microsoft Internet Explorer（已启用文档模式和浏览器模式）	9.0 10
Google Chrome	自 IBM Security QRadar V7.2.4 产品发布日期起的最新版本

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**。
   - 对于 Internet Explorer V9.0，选择 **Internet Explorer 9 标准**
   - 对于 Internet Explorer V8.0，选择 **Internet Explorer 8 标准**

访问 IBM Security QRadar Risk Manager 用户界面

IBM Security QRadar Risk Manager 为 URL、用户名和密码使用缺省登录信息。

通过 QRadar Console 访问 IBM Security QRadar Risk Manager。 登录 IBM Security QRadar Console 时，使用下表中的信息。

表 2. QRadar Risk Manager 的缺省登录信息

登录信息	缺省值
URL	https://<IP address>，其中 <IP address> 是 QRadar Console 的 IP 地址。
用户名	admin
密码	安装过程中分配给 QRadar Risk Manager 的密码。
许可证密钥	缺省的许可证密钥提供 5 周的系统访问权限。

设置 QRadar Risk Manager 设施

必须连接管理接口，并确保电源线插入到 QRadar Risk Manager 设施。

开始之前

阅读、理解和获取先决条件。

关于此任务

IBM Security QRadar Risk Manager 评估设施是一个两单元的机架装配服务器。 机架导轨与架子未随评估装置提供。

QRadar Risk Manager 设施包含四个网络接口。 对于本评估，请使用标注为 ETHO 的网络接口作为管理接口。 其他接口为监视接口。 所有接口都位于 QRadar Risk Manager 设施的后面板上。

电源按钮位于前面板上。

过程

1. 将管理网络接口连接到标注为 ETHO 的端口。
2. 确保将专用的电源线插到设施的尾部。
3. 可选。 要访问 QRadar SIEM 控制台，请连接 USB 键盘和标准 VGA 监视器。
4. 如果设施上带有前窗格，请按下任一侧的翼片并从设施上拉出，从而移除窗格。
5. 按下位于前面的电源按钮，将设施打开。

结果

设施开始引导过程。

将 QRadar Risk Manager 添加到 QRadar Console

必须将 IBM Security QRadar Risk Manager 作为受管主机添加到 IBM Security QRadar Console。

开始之前

如果要启用压缩，那么每个受管主机的最低版本必须是 QRadar Console 7.1 或 QRadar Risk Manager 7.1。

当控制台是 NAT 时，要将非 NAT 的受管主机添加到您的部署，必须将 QRadar Console 更改为 NAT 主机。 必须更改控制台，然后才能将受管主机添加到部署。 有关更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

过程

1. 打开 Web 浏览器。
2. 输入 URL `https://<IP Address>`，其中 <IP Address> 是 QRadar Console 的 IP 地址。
3. 输入用户名和密码。
4. 在**管理**选项卡上，单击**部署编辑器**。
5. 从菜单中，选择**操作**，然后选择**添加受管主机**。
6. 单击**下一步**。
7. 输入下列参数的值:

选项	描述
输入要添加的服务器或设施的 IP	QRadar Risk Manager 的 IP 地址。

选项	描述
输入主机的 root 密码	主机的 root 密码。
确认主机的 root 密码	确认密码。
主机是 NAT 的	要为受管主机启用 NAT，NAT 网络必须使用静态 NAT 转换。 有关更多信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。
启用加密	为主机创建 SSH 加密隧道。 要启用两个受管主机之间的加密，每个受管主机必须运行 QRadar Console 7.1 或 QRadar Risk Manager 7.1。
启用压缩	启用两个受管主机之间的数据压缩。

8. 选择下列其中一个选项:
   - 如果选择**主机是 NAT 的**复选框，那么必须输入 NAT 参数的值。

选项	描述
输入要添加的服务器或设施的 IP	受管主机的公共 IP 地址。 受管主机使用此 IP 地址，与其他网络中使用 NAT 的其他受管主机通信。
选择 NAT 网络	您希望该受管主机使用的网络。 如果受管主机位于与 QRadar Console 相同的子网上，那么选择 NAT 网络的控制台。 如果受管主机位于与 QRadar Console 不同的子网上，那么选择 NAT 网络的受管主机。

   - 如果未选择**主机是 NAT 的**复选框，则单击**下一步**。
9. 单击**完成**。 完成此过程可能要耗时几分钟。 如果您的部署包含了更改，您必须部署所有更改。
10. 单击**部署**。

下一步做什么

清除 Web 浏览器缓存，然后登录 QRadar Console。 现在**风险**选项卡就可用了。

建立通信

必须在 QRadar Risk Manager 设施和 QRadar SIEM 控制台之间建立通信，然后才能设置和配置 QRadar Risk Manager。

关于此任务

建立通信的过程可能要耗时几分钟完成。 如果要更改 QRadar Risk Manager 设施的 IP 地址，或者需要将 QRadar Risk Manager 连接到另一 QRadar SIEM 控制台，您可以使用 QRadar SIEM **管理**选项卡上的**Risk Manager 设置**。

过程

1. 打开 Web 浏览器，然后清除 Web 浏览器缓存。

2. 登录 QRadar SIEM。 有关 IP 地址、用户名或 root 密码的信息，请参阅访问 IBM Security QRadar Risk Manager 用户界面。
3. 单击**风险**选项卡。
4. 输入下列参数的值:

选项	描述
IP/主机	QRadar Risk Manager 设施的 IP 地址或主机名
Root 密码	QRadar Risk Manager 设施的 root 密码。

5. 单击**保存**。

下一步做什么

定义用户角色。

添加 Risk Manager 用户角色

必须分配 Risk Manager 用户角色，才能提供对 QRadar Risk Manager 的访问权限。

关于此任务

缺省情况下，QRadar SIEM 会提供一个缺省的管理角色，该角色可提供对 QRadar Risk Manager 中所有内容的访问权限。 被分配管理特权的用户（包括缺省的管理角色）不能编辑自己的帐户。 其他管理用户必须进行任何必要的更改。

有关创建和管理用户角色的信息，请参阅 *IBM Security QRadar SIEM Administration Guide*。

过程

1. 单击**管理**选项卡。
2. 在导航菜单中，单击**系统配置**。
3. 在**用户管理**窗格，单击**用户角色**。
4. 在左窗格中，选择要编辑的用户角色。
5. 选择 **Risk Manager** 复选框。
6. 单击**保存**
7. 单击**关闭**。
8. 在**管理**选项卡上，单击**部署更改**。

第 3 章 网络数据收集

必须配置 QRadar Risk Manager，以读取来自网络中设备的配置信息。

从网络设备收集的配置信息会生成网络的拓扑，并使 QRadar Risk Manager 能理解您的网络配置。

在 QRadar Risk Manager 中收集的数据，会连同与网络环境有关的关键信息填充拓扑。

数据收集是一个三步骤的过程:

- 向 QRadar Risk Manager 提供凭证，以下载网络设备配置。
- 发现设备，在“配置源管理”中创建设备列表。
- 备份设备列表以获取设备配置，并用与网络相关的数据填充拓扑。

凭证

必须使用凭证对 QRadar Risk Manager 进行配置，才能访问和下载设备配置。 凭证可使 QRadar Risk Manager 能连接到路由器、交换机或入侵防御系统 (IPS) 设备。

管理员可使用**配置源管理**输入设备凭证，这些凭证向 QRadar Risk Manager 提供了对特定设备的访问权。 QRadar Risk Manager 可为特定的网络设备保存单独的设备凭证。如果多个网络设备使用相同的凭证，您可将凭证分配到一个组。 例如，如果公司内所有防火墙具有相同的用户名和密码，您就可以将凭证分配到一个组。 这些凭证与所有防火墙的地址集相关联，用来备份公司内所有防火墙的设备配置。

注: 如果某个特定设备不需要网络凭证，则可在**配置源管理**中，将该参数保留为空。

配置凭证

可配置网络设备，以向 QRadar Risk Manager 提供对设备的访问权限。

过程

1. 单击**管理**选项卡。
2. 在导航菜单中，单击**插件**。
3. 在**Risk Manager** 窗格，**配置源管理**。
4. 在导航菜单中，单击**凭证**。
5. 在**网络组**窗格，单击**添加新的网络组**。
6. 输入网络组的名称，并单击**确定**。
7. 在**添加地址**字段，输入设备的 IP 地址，并单击**添加**。 为每个必须添加的地址重复此步骤。

   注: 确保您添加的地址显示在**添加地址**框旁边的“网络地址”部分。 请勿在**配置源管理**中重复添加其他网络组已有的设备地址。
   可以输入 IP 地址、IP 地址范围、CIDR 子网或通配符。 例如，要使用通配符可输入 10.1.*.*，或者要使用 CIDR 可输入 10.2.1.0/24。
8. 在**凭证**窗格，单击**添加新的凭证集**。

9. 输入新凭证集的名称，并单击**确定**。
10. 选择您创建的凭证集的名称，然后配置以下参数的值:

选项	描述
用户名	用于登录适配器的有效用户名。 对于适配器，用户名和密码需要拥有几个文件的访问权限，例如 rule.C、objects.C、implied_rules.C 和 Standard.PF。
密码	设备的密码。
启用密码	输入第二级认证的密码。 当凭证提示需要专家模式的用户凭证时，需要此密码。
SNMP 获取社区	可选
SNMPv3 认证用户名	可选参数。
SNMPv3 认证密码	可选参数。
SNMPv3 隐私密码	可选参数。 这是要用于对 SNMPv3 陷阱进行解密的协议。

11. 单击**确定**。

发现设备

发现过程通过使用您添加的凭证，而将网络设备添加到拓扑接口。

过程

1. 单击**管理**选项卡。
2. 在导航菜单中，单击**插件**。
3. 在 **Risk Manager** 部分，单击**配置源管理**。
4. 在导航菜单中，单击**发现设备**。
5. 输入 IP 地址或 CIDR 范围，以指定要发现的设备位置。
6. 单击**添加 (+)** 图标。
7. 如果要从定义的 IP 地址或 CIDR 范围搜索设备，可选择**从上面定义的地址搜寻网络**框。
8. 单击**运行**。

获取设备配置

备份设备以下载设备配置，以便 QRadar Risk Manager 能将设备信息包含在拓扑中。

开始之前

必须配置凭证集，然后才能下载设备配置。

关于此任务

可以备份单个设备或所有设备。

有关从**作业**选项卡安排设备配置的自动备份的信息，请参阅*IBM Security QRadar Risk Manager User Guide*。

过程

1. 单击**管理**选项卡。
2. 在导航菜单中，单击**插件**。
3. 在 **Risk Manager** 窗格，**配置源管理**。
4. 单击**设备**选项卡。
5. 要获得所有设备的配置，请在导航窗格中单击**备份所有**。 单击**是**继续。
6. 要获得特定设备的配置，可选择单个设备。 要选择多个设备进行备份，可按住 Ctrl 键不放。 单击**备份**。

导入设备

使用“设备导入”，可通过逗号分隔值文件 (.CSV)，将适配器及其网络 IP 地址的列表添加到配置源管理器。

设备导入列表可以包含多达 5000 个设备，但该列表必须在导入文件中，为每个适配器及其关联的 IP 地址包含一行。

例如，

```
<Adapter::Name 1>,<IP Address>
<Adapter::Name 2>,<IP Address>
<Adapter::Name 3>,<IP Address>
```

其中:

`<Adapter::Name>` 包含制造商和设备名称，例如 Cisco::IOS。

`<IP Address>` 包含该设备的 IP 地址，例如 191.168.1.1。

表 3. 设备导入示例

制造商	名称	示例 **<Adapter::Name>,<IP Address>**
检查点	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Cisco 安全设施	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS，10.1.1.3
Cisco	Nexus	Cisco::Nexus
Generic	SNMP	Generic::SNMP,10.1.1.8
Juniper 网络	Junos	Juniper::JUNOS,10.1.1.5

导入 CSV 文件

您可以使用逗号分隔值 (CSV) 文件，将主设备列表导入到“配置源管理”。

开始之前

如果您导入设备列表，然后又对 CSV 文件中的某个 IP 地址进行了更改，那么可能会不小心使得“配置源管理”列表中的某个设备发生重复。 因此，在重新导入主设备列表之前，请从“配置源管理”删除设备。

过程

1. 单击**管理**选项卡。
2. 在导航菜单中，单击**插件**。
3. 在**插件**窗格中，单击**设备导入**。
4. 单击**浏览**。
5. 找到 CSV 文件，单击**打开**。
6. 单击**导入设备**。

结果

如果显示错误，那么您需要复查 CSV 文件以纠正错误，并重新导入文件。 如果设备列表结构不正确或包含错误的信息，CSV 文件的导入可能失败。 例如，CSV 文件可能缺少冒号或命令，多个设备可能位于同一行上，或者适配器名称可能有拼写错误。

如果设备导入异常中止，那么 CSV 文件中的任何设备都不会添加到“配置源管理”中。

对设备导入进行故障诊断

如果您在尝试导入设备后收到错误消息，则可能是因为 CSV 文件的导入失败。

如果设备列表的结构不正确，则可能无法导入设备。例如，CSV 文件可能缺少冒号或命令，或者多个设备可能位于同一行上。

另外，如果设备列表包含错误的信息，导入也可能失败。 例如，某个适配器名称出现拼写错误。

如果设备导入异常中止，那么 CSV 文件中的任何设备都不会添加到“配置源管理”中。消息中会显示已安装适配器的有效适配器名称的列表。 如果显示了错误，那么您必须复查 CSV 文件以纠正所有错误。 纠正错误之后，您可以重新导入该文件。

第 4 章 管理审计

IBM Security QRadar Risk Manager 可帮助您回答一些问题，从而有助于简化网络安全策略与合规性需求的评估。

合规性审计对于安全性管理员而言，是必要而复杂的任务。 QRadar Risk Manager 可帮助您回答以下问题:

- 我的网络设备是如何配置的？
- 我的网络资源是如何进行通信的？
- 我的网络的脆弱点在何处？

用例: 配置审计

您可以将 QRadar Risk Manager 捕获的网络设备配置信息用于审计合规性，以及用于安排配置备份。

配置备份提供了用于为审计合规性记录设备更改的集中和自动的方法。 配置备份对配置更改进行归档，并提供历史参考；您可以捕获历史记录，或者将配置与另一网络设备进行比较。

QRadar Risk Manager 中的配置审计为您提供了以下选项:

- 网络设备配置的历史记录。
- 规范化视图，当您比较配置时，该视图显示设备更改。
- 用于在设备上搜索规则的设施。

设备的配置信息可从“配置源管理”中的设备备份进行收集。 每次 QRadar Risk Manager 备份设备列表时，它会归档设备配置的副本，以提供历史参考。 您安排“配置源管理”越频繁，您拥有的用于比较和历史参考的配置记录就越多。

查看设备配置历史记录

您可以查看网络设备的配置历史记录。

关于此任务

您可以查看已备份的网络设备的历史记录信息。 此信息可从**配置监视器**页面上的**历史记录**窗格中访问。 “历史记录”窗格提供了有关网络设备配置的信息，以及有关上次使用“配置源管理”备份网络配置的日期信息。

配置显示了为 QRadar Risk Manager 中的网络设备存储的文件类型。 常见的配置类型有:

- **标准元素文档** (SED)，它们是一些包含有关网络设备信息的 XML 数据文件。各个 SED 文件可通过其原始 XML 格式查看。 如果一个 SED 文件与另一个 SED 文件进行比较，那么会对视图进行规范化处理，以显示规则差别。
- **Config**，它们是某些网络设备提供的配置文件。 这些文件取决于设备制造商。 可通过双击 config 文件来查看配置文件。

注: 根据您的设备，可能会显示其他几个配置文件。 双击这些文件，会以纯文本显示其内容。 纯文本视图支持 Web 浏览器窗口中的查找 (Ctrl+f)、粘贴 (Ctrl+v) 和复制 (Ctrl+C) 功能。

过程

1. 单击**风险**选项卡。
2. 在导航菜单中，单击**配置监视器**。
3. 双击配置可查看详细的设备信息。
4. 单击**历史记录**。
5. 在**历史记录**窗格，选择配置。
6. 单击**查看选定的**。

比较单个设备的设备配置

您可以比较单个设备的设备配置。

关于此任务

如果比较的文件是标准元素文档 (SED)，那么可以查看配置文件之间的规则差别。

比较规范化的配置时，文本颜色指示以下规则:

- 绿色点虚线轮廓线指示添加到设备的规则或配置。
- 红色短划虚线轮廓线指示已从设备删除的规则或配置。
- 黄色实线轮廓线设备上已修改的规则或配置。

过程

1. 单击**风险**选项卡。
2. 在导航菜单中，单击**配置监视器**。
3. 双击任意设备可查看详细的配置信息。
4. 单击**历史记录**可查看该设备的历史记录。
5. 选择主配置。
6. 按住 Ctrl 键，并选择要比较的第二个配置。
7. 在**历史记录**窗格上，单击**比较选定的**。
8. 可选。 要查看原始配置差别，请单击**查看原始比较**。 如果比较是针对 config 文件或另一备份类型，则会显示原始比较。

比较不同设备的设备配置

您可以比较不同设备的两种配置。

关于此任务

如果比较的文件是标准元素文档 (SED)，那么可以查看配置文件之间的规则差别。

比较规范化的配置时，文本颜色指示以下规则:

- 绿色点虚线轮廓线指示添加到设备的规则或配置。
- 红色短划虚线轮廓线指示已从设备删除的规则或配置。

- 黄色实线轮廓线设备上已修改的规则或配置。

过程

1. 单击**风险**选项卡。
2. 在导航菜单中，单击**配置监视器**。
3. 双击任意设备可查看详细的配置信息。
4. 单击**历史记录**可查看该设备的历史记录。
5. 选择主配置。
6. 单击**标记进行比较**。
7. 从导航菜单，选择**所有设备**以返回设备列表。
8. 双击要比较的设备，并单击**历史记录**。
9. 选择另一配置备份，与已标记的配置进行比较。
10. 单击**与已标记的进行比较**。
11. 可选。 要查看原始配置差别，请单击**查看原始比较**。 如果比较是针对 config 文件或另一备份类型，则会显示原始比较。

用例: 查看拓扑中的网络路径

QRadar Risk Manager 中的拓扑以图形表示法的方式显示网络设备。

拓扑路径搜索可以确定网络设备进行通信的方式，以及用来进行通信的网络路径。 路径搜索使得 QRadar Risk Manager 能直观地显示源和目标之间的路径，并且带有端口、协议和规则。

您可以查看设备如何通信，这对于受保护或受限制的访问资产是很重要的。

关键功能包括:

- 能够查看网络上设备之间的通信。
- 使用过滤器在拓扑中搜索网络设备。
- 快速访问以查看设备规则和配置。
- 能够查看从路径搜索生成的事件。

搜索拓扑

您可以通过搜索拓扑来查看设备通信。

关于此任务

可将路径搜索用于过滤拓扑模型。 路径搜索包括: 所有包含源 IP 地址或 CIDR 范围的网络子网; 包含目标 IP 地址或 CIDR 范围，且也允许使用已配置的协议和端口进行通信的子网。 搜索会检查您现有的拓扑模型，并包括源和目标之间通信路径所涉及的设备，以及详细的连接信息。

如果拓扑包括了入侵预防系统 (IPS)，您可以使用脆弱性来过滤搜索。 有关更多信息，请参阅 *IBM Security QRadar Risk Manager User Guide*。

过程

1. 单击**风险**选项卡。
2. 在导航菜单中，单击**拓扑**。
3. 从**搜索**列表框，选择**新建搜索**。
4. 在**搜索条件**窗格中，选择**路径**。
5. 在**源 IP/CIDR** 字段，输入要在上面过滤拓扑模型的 IP 地址或 CIDR 范围。 用逗号分隔多个条目。
6. 在**目标 IP/CIDR** 字段，输入要在上面过滤拓扑模型的目标 IP 地址或 CIDR 范围。 用逗号分隔多个条目。
7. 可选。 从**协议**列表，选择要用来过滤拓扑模型的协议。
8. 可选。 在**目标端口** 字段，输入要在上面过滤拓扑模型的目标端口。 用逗号分隔多个端口。
9. 单击**确定**。
10. 将鼠标移至连接线上方，可查看关于连接的详细信息。 如果搜索连接到包含规则的设备，则会在对话框中显示设备规则链接。

用例: 查看攻击的攻击路径

QRadar Risk Manager 中的攻击是由系统生成的事件，用来警告您网络出现状况或事件。

攻击路径可视化将攻击与拓扑搜索联系在了一起。这种可视化使得安全性操作员能查看攻击详细信息，以及攻击在网络中采用的路径。 攻击路径为您提供了直观的表示。 这种直观的表示向您展现了网络中的一些资产，这些资产正在进行通信而使得攻击可穿越网络。 此数据在审计期间非常关键，可证明您在对攻击进行监视，但同时也证明该攻击在网络中没有指向关键资产的备用路径。

可视化的关键功能有:

- 利用 QRadar SIEM 中的现有规则和攻击系统。
- 为所有设备显示攻击源与目标之间的可视路径。
- 快速访问允许该攻击的设备配置和规则。

查看攻击的攻击路径

您可以查看攻击的攻击路径。 攻击路径显示了源、目标与关联设备。

过程

1. 单击**攻击**选项卡。
2. 在导航菜单中，单击**所有攻击**。 **所有攻击**页面显示网络中攻击的列表。 攻击列出时，量级最高的攻击列在最前面。
3. 双击攻击，可打开攻击摘要。
4. 在**攻击**工具栏，单击**查看攻击路径**。

第 5 章 用例: 监视策略

策略审计和更改控制是一些基本流程，它们使管理员和安全专家能控制关键业务资产之间的访问和通信。

策略监视的条件可以包括以下场景中的资产和通信监视:

- 对于 PCI 部分 1 审计，我的网络是否包含具有高风险配置的资产？
- 对于 PCI 部分 10 审计，我的资产是否允许使用高风险协议进行通信？
- 当策略更改使得我的网络出现违例时，我如何能知晓？
- 我如何查看硬化资产或高风险资产的脆弱性？
- 我如何查看网络中具有脆弱性和互联网访问权限的资产？

使用策略监视器定义基于风险指示器的测试，然后对测试结果进行限定，以过滤特定结果、违例、协议或脆弱性的查询。

IBM Security QRadar Risk Manager 包含按 PCI 类别分组的几个策略监视器问题。 例如 PCI 1、PCI 6 和 PCI 10 问题。 可以为资产或设备与规则创建问题，以暴露网络安全性风险。 在将关于资产或设备/规则的问题提交到策略监视器之后，返回的结果会指定风险级别。 您可批准从资产返回的结果，也可定义希望系统响应未批准结果的方式。

策略监视器提供了以下关键功能:

- 预定义策略监视器问题，用以协助工作流程。
- 确定用户是否使用了禁止的协议进行通信。
- 评估特定网络上的用户是否能与禁止的网络或资产通信。
- 评估防火墙规则是否符合公司策略。
- 持续地对为管理员生成攻击或警报的策略进行监视。
- 通过评估哪些系统的安全性因设备配置而受到威胁，来划分脆弱性的优先级。
- 帮助识别合规性问题。

用例: 评估具有可疑配置的资产

组织使用公司安全性策略，来定义风险以及资产和网络之间允许的通信。为帮助了解合格与公司策略违规的情况，组织使用策略监视器来评估和监视可能未知的风险。

PCI 合规性规定，您识别包含持卡人数据的设备，然后绘图、验证通信以及监视防火墙配置，以保护含有敏感数据的资产。策略监视器提供了快速满足这些需求的方法，并使管理员能遵守公司策略。 降低风险的常见方法包括，识别并监视使用未受保护的协议进行通信的资产。 这些协议的例子有允许 FTP 或 telnet 连接的路由器、防火墙或交换机。使用策略监视器可识别拓扑中具有高风险配置的资产。

PCI 部分 1 问题可包括以下条件:

- 允许已禁止协议的资产。
- 允许高风险协议的资产。

- 允许跨网络的策略外应用程序的资产。
- 允许包含受保护资产的网络上有策略外应用程序的资产。

对允许高风险协议的设备进行评估

使用策略监视器，对允许高风险协议的设备进行评估。

关于此任务

QRadar Risk Manager 对问题进行评估，并将拓扑中与测试问题相匹配的所有资产的结果显示出来。 网络中的安全性专家、管理员或审计员可以批准对特定资产不具有风险的通信。 他们还能为行为创建攻击。

过程

1. 单击**风险**选项卡。
2. 在导航菜单中，单击**策略监视器**。
3. 从“组”列表框，选择 **PCI 1**。
4. 选择测试问题**对从互联网到 DMZ 的允许高风险协议（即 telnet 和 FTP 流量 - 分别为端口 21 和 23）的任何设备（即防火墙）进行评估**。
5. 单击**提交问题**。

用例: 评估具有可疑通信的资产

通过跟踪、记录和显示对网络资产的访问，使用策略监视器识别 PCI 部分 10 合规性。

QRadar Risk Manager 可通过识别拓扑中允许进行有问题或高风险通信的资产，而帮助识别 PCI 部分 10 合规性。 QRadar Risk Manager 可针对实际的通信或可能的通信来检查这些资产。实际的通信显示使用了您的问题条件进行通信的资产。 可能的通信则显示可能使用您的问题条件进行通信的资产。

PCI 部分 10 问题可包括以下条件:

- 允许问题进入内部网络的资产。
- 从不受信任位置传播到受信任位置的资产。
- 从 VPN 传播到受信任位置的资产。
- 允许受信任位置内部出现未加密策略外协议的资产。

查找允许通信的资产

您可以查找允许来自互联网的通信的资产。

关于此任务

QRadar Risk Manager 对问题进行评估，并显示允许来自互联网入站连接的任何内部资产的结果。 安全性专家、管理员或网络审计员可以批准对被认为不安全的资产或包含客户数据的资产进行访问的权利。随着所生成事件的增多，您可以在 QRadar SIEM 中创建攻击来监视此类具有风险的通信。

过程

1. 单击**风险**选项卡。
2. 在导航菜单中，单击**策略监视器**。
3. 从“组”列表框，选择 **PCI 10**。
4. 选择测试问题**评估从互联网到内部网任何位置的所有入站连接**。
5. 单击**提交问题**。

用例: 监视违例策略

QRadar Risk Manager 能在策略监视器中持续地监视任何预定义或用户生成的问题。 您可使用监视模式，在 QRadar Risk Manager 中生成事件。

如果选择了要监视的问题，QRadar Risk Manager 会根据拓扑每小时分析问题，以确定资产或规则更改是否生成了未经批准的结果。 如果 QRadar Risk Manager 检测到未经批准的结果，则会生成一个攻击，以警告您与确定的策略存在偏差。 在监视模式下，QRadar Risk Manager 能同时监视 10 个问题的结果。

问题监视提供了以下关键功能:

- 每小时监视规则或资产更改以发现未经批准的结果。
- 使用高级别和低级别事件类别，将未经批准的结果分类。
- 对未经批准的结果生成攻击、电子邮件、系统日志消息或仪表板通知。
- 在 QRadar SIEM 中使用事件查看、关联、事件报告、定制规则和仪表板。

配置问题

可使用策略监视器来配置要监视的问题。

过程

1. 单击**风险**选项卡。
2. 在导航菜单中，单击**策略监视器**。
3. 选择要监视的问题。
4. 单击**监视**。
5. 配置监视问题时需要的任何选项。
6. 单击**保存监视器**。

结果

这样就为问题启用了监视，并基于您的监视条件生成事件或攻击。

用例: 使用脆弱性对风险划分优先级

暴露的脆弱性对于网络资产是一项重大的风险因素。

QRadar Risk Manager 利用了策略监视器中的资产信息和脆弱性信息。这些信息用来确定资产是否易受输入型的攻击，例如: SQL 注入、隐藏字段以及点击劫持。

对于在资产上检测到的脆弱性，可以根据其网络位置或与其他脆弱设备的连接性来划分优先级。

脆弱性资产问题可包括以下条件:

- 特定日期之后报告了新的脆弱性的资产。
- 具有特定脆弱性或 CVSS 得分的资产。
- 具有特定脆弱性分类的资产，例如输入操作、服务拒绝以及已验证的 OSVDB。

查找具有脆弱性的资产

您可以查找具有脆弱性的资产。

关于此任务

QRadar Risk Manager 对问题进行评估，并显示包含脆弱性的资产结果。 安全性专家、管理员或审计员可以识别网络中包含已知 SQL 注入脆弱性的资产。 他们能迅速地修补与受保护网络连接的任何资产。 随着所生成事件的增多，您可以在 QRadar SIEM 中创建事件或攻击，来监视包含 SQL 注入脆弱性的资产。

过程

1. 单击**风险**选项卡。
2. 在导航菜单中，单击**策略监视器**。
3. 从**组**列表，选择**脆弱性**。
4. 选择测试问题**对特定局域网（即受保护服务器网络）上具有 SQL 注入脆弱性的资产进行评估**。
5. 单击**提交问题**。

用例: 按区域或网络通信划分资产脆弱性优先级

与受保护资产位于同一网络中具有脆弱性的系统，其数据丢失的风险更高。

按区域或网络检测资产的脆弱性，是阻止网络中出现开采的关键措施。 PCI 部分 6.1 和 6.2 规定，应当在脆弱性补丁发布后一个月内，复查并修补系统。 QRadar Risk Manager 有助于修补过程的自动化和优先级划分。 当检测出资产存在脆弱性之后，您可以根据网络位置或与其他脆弱设备的连接性来划分优先级。 对于可连接到可疑区域的受保护网络，或者 CVSS 得分高于内部策略允许值的资产，划分优先级很重要。

脆弱资产问题可包括以下条件:

- 具有客户端脆弱性的资产，其与可疑地理区域通过信，并包含受保护资产。
- 在特定网络中拒绝服务脆弱性的资产。
- 在特定网络中具有邮件脆弱性的资产。
- 具有脆弱性和特定的公共脆弱性评分系统 (CVSS) 得分的资产。

查找网络中具有脆弱性的资产

您可以查找特定网络中具有脆弱性的资产。

关于此任务

Qradar Risk Manager 对问题进行评估，并将结果显示在包含特定于操作系统脆弱性的特定位置。 安全性专家、管理员或网络审计员可以批准对被认为不安全的资产或包含

客户数据的资产进行访问的权利。 随着所生成事件的增多，您可以创建攻击来监视此类具有风险的通信。

过程

1. 单击**风险**选项卡。
2. 在导航菜单中，单击**策略监视器**。
3. 从**组**列表框，选择**脆弱性**。
4. 选择测试问题**对特定局域网上具有特定于操作系统脆弱性的资产进行评估**。
5. 单击**提交问题**。

第 6 章 模拟的用例

用例: 模拟对网络资产的攻击

您可以使用模拟，以测试您的网络对于各种来源的脆弱性。

您可以使用攻击模拟，以审核网络中的设备配置。

模拟提供了以下关键功能:

- 模拟显示对网络进行攻击时可采取的理论路径排列。
- 模拟显示攻击如何能在网络设备中传播而扩散到其他资产。
- 模拟允许进行监视，以检测新的暴露站点。

创建模拟

可以在 SSH 协议上创建网络攻击的模拟。

过程

1. 单击**风险**选项卡。
2. 在导航菜单中，选择**模拟 > 模拟**。
3. 从**操作**列表，选择**新建**。
4. 输入模拟的名称。
5. 选择**当前拓扑**。
6. 选择**使用连接数据**复选框。
7. 从**您要从哪里开始模拟**列表，选择模拟的源。
8. 添加模拟攻击，**攻击瞄准其中一个以下使用协议的开放端口**。
9. 对于本模拟，单击**开放端口**，然后添加端口 22。
10. 单击**协议**，然后选择 **TCP**。 SSH 使用 TCP。
11. 单击**确定**。
12. 单击**保存模拟**。
13. 从**操作**列表，选择**运行模拟**。 结果列包含一个列表，该列表由模拟运行的日期及用来查看模拟结果的链接组成。
14. 单击**查看结果**。

结果

一个包含 SSH 脆弱性的资产列表会显示在结果中，使得网络管理员能审批网络中允许或期望出现的 SSH 连接。 可以对未经批准的连接进行监视，以发现事件或攻击。

通过显示的结果，网络管理员或安全专家可直观地了解攻击在网络中可能采用的攻击路径和连接。例如，第一步提供了受模拟影响的直接连接资产的列表。 第二步列出了网络中能与模拟中第一级资产进行通信的资产。

攻击中提供的信息使您能够针对数千种可能的攻击场景，来强化和测试您的网络。

用例: 模拟网络配置更改的风险

可以使用拓扑模型，基于现有网络来定义虚拟网络模型。 可以创建网络模型，该模型基于一系列可以组合和配置的修改。

可以使用拓扑模型，通过模拟来确定配置更改对网络的影响。

拓扑模型提供以下关键功能:

- 创建虚拟拓扑，以测试网络更改。
- 模拟对虚拟网络的攻击。
- 通过测试降低受保护资产的风险和暴露。
- 虚拟网络分段使您能够限定网络或资产的敏感部分，并进行测试。

要模拟网络配置更改:

1. 创建拓扑模型。
2. 模拟对拓扑模型的攻击。

创建拓扑模型

可以创建拓扑模型以测试网络更改并模拟攻击。

过程

1. 单击**风险**选项卡。
2. 在导航菜单中，选择**模拟 > 拓扑模型**。
3. 从**操作**列表，选择**新建**。
4. 输入模型的名称。
5. 选择您要应用到拓扑的所有修改。
6. 对添加到**如下配置模型**窗格的测试进行配置。
7. 单击**保存模型**。

下一步做什么

为新的拓扑模型创建模拟。

模拟攻击

您可以模拟对端口和协议的攻击。

过程

1. 单击**风险**选项卡。
2. 在导航菜单中，选择**模拟 > 模拟**。
3. 从**操作**列表框，选择**新建**。
4. 输入模拟的名称。
5. 选择一个您创建的拓扑模型。
6. 从**您要从哪里开始模拟**列表，选择模拟的源。
7. 添加模拟攻击，**攻击瞄准其中一个以下使用协议的开放端口**。
8. 对于本模拟，单击**开放端口**，然后添加端口 22。

9. 单击**协议**，然后选择 TCP。 SSH 使用 TCP。
10. 单击**确定**。
11. 单击**保存模拟**。
12. 从**操作**列表，选择**运行模拟**。 结果列包含一个列表框，该列表框由模拟运行的日期及用来查看模拟结果的链接组成。
13. 单击**查看结果**。

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 公司可能已拥有或正在申请与本文档所述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。

本资料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 Customer Agreement、IBM 客户协议、IBM 国际软件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资料中获取。 IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。 有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

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。

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 Corporation 在美国和/或其他国家或地区的商标或注册商标。 如果这些商标或注册商标以及其他 IBM 商标项在本文档中第一次出现时标注了商标符号（® 或 ™），则这些符号表示在本文档发布时，IBM 已拥有的美国注册商标或普通法商标。 此类商标也可能是在其他国家或地区的注册商标或普通法商标。 IBM 商标的最新列表可从以下 Web 站点获得 Copyright and trademark information (www.ibm.com/legal/copytrade.shtml)。

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。

其他的公司、产品和服务名称可能是其他公司的商标或服务标志。

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）。

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

索引

I

M

N

P

R

S

W