IBM Security QRadar Risk Manager
バージョン 7.2.6

ユーザー・ガイド

IBM

注記

本書および本書で紹介する製品をご使用になる前に、 175 ページの『特記事項』に記載されている情報をお読みください。

この資料は、IBM QRadar Security Intelligence Platform V7.2.6 に適用されます。また、この資料の更新版が公開されない限り、これ以降のリリースにも適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM Security QRadar Risk Manager
Version 7.2.6
User Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

© Copyright IBM Corporation 2012, 2015.

目次

© Copyright IBM Corp. 2012, 2015

IBM Security QRadar Risk Manager の概要

この情報は、IBM® Security QRadar® Risk Manager で利用されることを目的としています。QRadar Risk Manager は、デバイス構成のモニター、ネットワークの変更のシミュレーション、およびネットワーク内のリスクと脆弱性の優先順位付けに使用するアプライアンスです。

このガイドでは、IBM Security QRadar Risk Manager を IBM Security QRadar SIEM コンソールで構成して使用する手順を説明しています。

対象読者

QRadar Risk Manager の構成および使用を担当するシステム管理者には、IBM Security QRadar SIEM およびネットワーク・デバイスとファイアウォールに対する管理アクセス権限が必要です。また、システム管理者には、企業ネットワークとネットワーキング・テクノロジーに関する知識が必要です。

技術資料

詳細な技術資料、技術情報、およびリリース情報にアクセスする方法については、Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861) を参照してください。

お客様サポートへのお問い合わせ

お客様サポートへのお問い合わせについては、Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861) を参照してください。

適切なセキュリティーの実践に関する注意事項

IT システム・セキュリティーには、企業内外からの不正アクセスの防止、検出、および対応によって、システムや情報を保護することが求められます。不正なアクセスにより、情報の改ざん、破壊、盗用、悪用が発生したり、使用しているシステムの損傷や、他のシステムに対する攻撃のための利用を含む悪用につながる可能性があります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

© Copyright IBM Corp. 2012, 2015

第 1 章 QRadar Risk Manager V7.2.6 のユーザー用の新機能

IBM Security QRadar Risk Manager V7.2.6 では、ネットワーク・トポロジーの整理と管理、ユーザーおよびグループによるデバイス・ルールのフィルター操作、および新規デバイスの統合のための機能拡張が行われています。

トポロジー画面の機能拡張

デバイスのグループ化、デバイスの名前変更、デバイスごとに表示するサブネットの数のフィルター操作、分類していないデバイスの表示または非表示によってトポロジー・グラフの管理や整理を行います。デバイスおよびサブネットをフィルターに掛けてグラフを整理することで、ネットワーク・ノード表示の混雑の程度を管理できます。  詳細...

ユーザーまたはグループによるデバイス・ルールのフィルター操作

ネットワーク・ルール・ポリシーの管理と最適化を容易にするために、ユーザーまたはグループによってデバイス・ルールを表示、フィルター操作、および検索することができます。  詳細...

アダプターの統合

QRadar Risk Manager には、サポートされているネットワーク・デバイス (応答可能なファイアウォール、ルーター、スイッチなど) を拡張する 2 つの新しいアダプター統合が導入されています。

Sidewinder アダプター

Sidewinder 用の QRadar Risk Manager アダプターは、SecureOS を実行する McAfee Enterprise Firewall (Sidewinder) アプライアンスをサポートしています。

TippingPoint アダプター

TippingPoint 用の QRadar Risk Manager アダプターは、TOS を実行し、かつ SMS 管理下にある TippingPoint アプライアンスをサポートしています。

詳しくは、「*IBM Security QRadar Risk Manager Adapter Configuration Guide*」を参照してください。

© Copyright IBM Corp. 2012, 2015

第 2 章 IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager は、デバイス構成のモニター、ネットワーク環境に対する変更のシミュレート、およびネットワーク内のリスクおよび脆弱性の優先順位付けを行うための、別個にインストールされるアプライアンスです。

QRadar Risk Manager にアクセスするには、IBM Security QRadar SIEM コンソールで「**リスク**」タブを使用します。

QRadar Risk Manager は、QRadar によって収集されたデータを使用します。例えば、ファイアウォール、ルーター、スイッチ、また侵入防止システム (IPS)、脆弱性フィード、およびサード・パーティーのセキュリティー・ソースから得られる構成データです。データ・ソースにより、QRadar Risk Manager はネットワーク内のセキュリティー、ポリシー、およびコンプライアンスのリスクを識別し、リスクが悪用される確率を推定することが可能になります。

QRadar Risk Manager は、「**オフェンス**」タブにオフェンスを表示して、検出したリスクのアラートを通知します。リスク・データは、QRadar が処理するその他のすべてのデータのコンテキストで分析され、レポートされます。 QRadar Risk Manager では、企業のリスク許容度に基づいた許容レベルでリスクを評価および管理できます。

また、QRadar Risk Manager を使用して、すべてのネットワーク接続の照会、デバイス構成の比較、ネットワーク・トポロジーのフィルタリング、およびデバイス構成の更新によって発生する可能性のある影響のシミュレーションを行うことができます。

QRadar Risk Manager を使用して、ネットワークに関するポリシー (または質問) のセットを定義したり、それらのポリシーをモニターして、変更を検出したりすることができます。例えば、インターネットからの暗号化されていないプロトコルを DMZ で拒否するには、暗号化されていないプロトコルを検出するためのポリシー・モニターの質問を定義できます。質問を送信すると、インターネットから DMZ に通信している、暗号化されていないプロトコルのリストが返され、セキュリティー・リスクとなる暗号化されていないプロトコルを判別できます。

接続

「接続」ページを使用して、ローカル・ホストのネットワーク接続をモニターします。

ローカル・ホストが通信可能なアプリケーション、ポート、プロトコル、および Web サイトに基づき、ローカル・ホストのネットワーク接続の照会およびレポートを実行できます。

接続について詳しくは、接続の調査を参照してください。

© Copyright IBM Corp. 2012, 2015

構成モニター

構成モニターを使用して、デバイス構成を検討および比較します。これにより、セキュリティー・ポリシーを適用したり、ネットワーク内のデバイスの変更をモニターしたりできます。

デバイス構成には、ネットワーク内のスイッチ、ルーター、ファイアウォール、および IPS デバイスが含まれることが考えられます。それぞれのデバイスについて、デバイスの構成履歴、インターフェース、ルールを表示できます。また、単一のデバイスおよび複数のデバイスで構成を比較することもできます。

デバイス構成情報を使用して全社的なネットワーク・トポロジーの表示を作成することもできます。こうすることで、ネットワーク全体で許可されるアクティビティーと拒否されるアクティビティーを決定できます。デバイス構成で、ネットワークにリスクをもたらす矛盾や構成変更を識別できるようになります。

トポロジー

トポロジーは、構成ソース管理から追加したデバイスに基づいてネットワークのネットワーク層をグラフィカル表現したものです。

ネットワーク層は開放型システム間相互接続 (OSI) モデルの第 3 層です。

アプリケーション層は OSI モデルの第 7 層です。

デバイス間の接続、複数のコンテキストを持つ仮想ネットワーク・セキュリティー・デバイス、アセット、ネットワーク・アドレス変換 (NAT) デバイス、NAT インディケーター、および NAT マッピングについての情報を表示するには、トポロジーの対話式グラフを使用します。

イベント、デバイス、パスを検索したり、ネットワーク・レイアウトを保存したりすることができます。

デバイスをグループ化したり、デバイスやグループを名前変更したりすることができます。

トポロジーでは、トランスポート層 (第 4 層) を照会して、ポートやプロトコルに基づいてネットワーク・パスをフィルターに掛けることができます。グラフおよび接続情報は、ネットワーク・デバイス (ファイアウォール、ルーター、侵入防止システム (IPS) など) から取得した詳細な構成情報から作成されます。

詳しくは、トポロジーを参照してください。

ポリシー・モニター

ポリシー・モニターを使用して、ネットワーク内のリスクに関する具体的な質問を定義し、その質問を IBM Security QRadar Risk Manager に送信します。

QRadar Risk Manager は、ユーザーによって質問に定義されたパラメーターを評価し、ネットワーク内の該当するアセットを返して、ユーザーがリスクを評価できるようにします。質問のベースとなる一連のテストは、必要に応じて組み合わせて構

成することができます。QRadar Risk Manager には多数の定義済みポリシー・モニターの質問が用意され、カスタム質問を作成できます。以下のシチュエーションについてポリシー・モニターの質問を作成できます。

- 発生した通信
- ファイアウォールおよびルーターの構成に基づく潜在的通信
- 実際のファイアウォール・ルール (デバイス・テスト)

ポリシー・モニターは、構成データ、ネットワーク・アクティビティー・データ、ネットワーク・イベントとセキュリティー・イベント、および脆弱性スキャン・データから取得されたデータを使用して、適切な応答を決定します。
PCI、HIPPA、ISO 27001 などの複数の規制要件および機密保護のベスト・プラクティス全体でリスクの判断を支援するために、QRadar Risk Manager にはポリシー・テンプレートが用意されています。企業が定義している機密保護ポリシーに合わせて、これらのテンプレートを更新できます。応答が完了したら、質問に対する応答を受け入れて、許容できない結果に対するシステムの応答方法を定義することができます。

ポリシー・モニターでアクティブにモニターできる質問の数に制限はありません。質問のモニター時に QRadar Risk Manager は質問を継続的に評価し、承認されていない結果がないかを調べます。承認されない結果を検出したとき、QRadar Risk Manager は E メールの送信、通知の表示、syslog イベントの生成、または IBM Security QRadar SIEM でのオフェンスの作成を行うことができます。

ポリシー・モニターについて詳しくは、ポリシー・モニターを参照してください。

シミュレーション

ネットワークでのエクスプロイト・シミュレーションを定義し、スケジュールして実行するには、シミュレーションを使用します。

ポリシー・モニターの場合と同様の方法で構成した一連のパラメーターに基づいて、ご使用のトポロジーに対する攻撃のシミュレーションを作成することができます。現在のネットワーク・トポロジーに対する攻撃のシミュレーションを作成したり、トポロジー・モデルを作成したりすることができます。トポロジー・モデルは仮想的なトポロジーであり、この仮想トポロジーに対して変更を加えて攻撃をシミュレートすることができます。これにより、ネットワーク・ルール、ポート、プロトコル、許可される接続、または拒否される接続を変更した場合にネットワークに及ぶ影響をシミュレートすることができます。シミュレーションは強力なツールであり、ネットワーク構成に対して計画している変更を実際に適用する前に、その変更によるリスクの影響を判断することができます。

シミュレーションが完了した後、結果を検討することができます。結果を受け入れる場合は、シミュレーション・モードを構成して、許容できない結果に対する対処方法を定義することができます。

IBM Security QRadar Risk Manager でアクティブにモニターできるシミュレーションは 10 件までです。シミュレーションをモニターするときに、QRadar Risk Manager は、継続的にトポロジーを分析して、承認されない結果が発生するかどう

か監視します。承認されない結果を検出したとき、QRadar Risk Manager は、E メールの送信、通知の表示、syslog イベントの生成、または QRadar SIEM でのオフェンスの作成を行うことができます。

シミュレーションについて詳しくは、シミュレーションの使用を参照してください。

IBM Security QRadar Risk Manager レポート

「**レポート**」タブを使用して、QRadar Risk Manager で使用可能なデータ (接続、デバイス・ルール、デバイス未使用オブジェクトなど) に基づいた、特定のレポートを表示します。

さらに以下の詳細レポートも使用できます。

- デバイス間の接続
- デバイス上のファイアウォール・ルール
- デバイス上の未使用オブジェクト

レポートについて詳しくは、IBM Security QRadar Risk Manager レポートの管理を参照してください。

サポート対象の Web ブラウザー

IBM Security QRadar 製品の機能が正しく動作するためには、サポート対象の Web ブラウザーを使用する必要があります。

QRadar システムにアクセスすると、ユーザー名とパスワードの入力を求められます。このユーザー名とパスワードは、管理者が事前に構成しておく必要があります。

以下の表に、サポートされる Web ブラウザーのバージョンをリストします。

表 1. QRadar 製品でサポートされる Web ブラウザー

Web ブラウザー	**サポートされるバージョン**
Mozilla Firefox	38.0 延長サポート版
32 ビット版の Microsoft Internet Explorer (ドキュメント・モードおよびブラウザー・モードを有効にすること)	10.0 11.0
Google Chrome	バージョン 43 以前。

Internet Explorer でのドキュメント・モードおよびブラウザー・モードの有効化

Microsoft Internet Explorer を使用して IBM Security QRadar 製品にアクセスする場合は、ドキュメント・モードおよびブラウザー・モードを有効にする必要があります。

手順

1. Internet Explorer Web ブラウザーで、F12 を押して「開発者ツール」ウィンドウを開きます。
2. 「**ブラウザー モード**」をクリックし、ご使用の Web ブラウザーのバージョンを選択します。
3. 「**ドキュメント モード**」をクリックし、ご使用の Internet Explorer リリースの「**Internet Explorer 標準 (Internet Explorer standards)**」を選択します。

IBM Security QRadar Risk Manager ユーザー・インターフェースへのアクセス

IBM Security QRadar Risk Manager は、URL、ユーザー名、パスワードに関するデフォルトのログイン情報を使用します。

QRadar Risk Manager には IBM Security QRadar SIEM コンソール からアクセスします。 QRadar コンソール にログインする場合は、以下の表の情報を参照してください。

表 2. QRadar Risk Manager のデフォルト・ログイン情報

ログイン情報	デフォルト
URL	https://<IP address> (<*IP address*> は、QRadar コンソール の IP アドレスです)。
ユーザー名	admin
パスワード	インストール・プロセスで QRadar Risk Manager に割り当てられたパスワード。
ライセンス・キー	デフォルトのライセンス・キーを使用すると、システムに 5 週間アクセスすることができます。

IBM Security QRadar Risk Manager でサポートされない機能

QRadar Risk Manager でサポートされない機能を把握しておくことは重要です。

以下の機能は QRadar Risk Manager でサポートされていません。

- 高可用性 (HA)
- Border Gateway Protocol (BGP)、Open Shortest Path First (OSPF)、または Routing Information Protocol (RIP) の場合の動的ルーティング
- IPv6
- 不連続なネットワーク・マスク
- ロード・バランスされる経路
- リファレンス・マップ
- ストア・アンド・フォワード

第 3 章 QRadar Risk Manager へのアクセスの構成

QRadar Risk Manager に対するアクセス設定は、IBM Security QRadar SIEM の「**管理**」タブで構成できます。QRadar Risk Manager をデプロイメント環境に追加する際は、ローカル・ファイアウォール、ネットワーク・インターフェース、E メール・サーバーなどの設定を構成し、適切なライセンスを追加する必要があります。

管理者権限を持っている場合、QRadar Risk Manager 用のいくつかのアプライアンス設定を構成できます。

管理者は、以下のタスクを行うことができます。

- 「システムおよびライセンス管理」ウィンドウで、QRadar Risk Manager 用にライセンスの管理、ローカル・ファイアウォールの構成、E メール・サーバーの追加、およびネットワーク・インターフェースの構成を行う。
- ホストのパスワードを変更する。
- システム時刻を更新する。

ファイアウォール・アクセスの構成

IBM Security QRadar Risk Manager のローカル・ファイアウォールを構成して、このホストにアクセスする必要がある、デプロイメント外部の指定デバイスからのアクセスを許可します。例えば、QRadar セットアップの一部ではないコンピューターからこのホストに接続することができます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**システム構成**」をクリックします。
3. 「**システムおよびライセンス管理**」アイコンをクリックします。
4. 「**表示**」メニューから、「**システム**」を選択します。
5. ファイアウォール・アクセス設定の構成対象となるホストを選択します。
6. 「**アクション**」メニューから、「**システムの表示と管理**」をクリックします。

   選択したホストを右クリックしてこのメニュー・オプションにアクセスするか、またはホストをダブルクリックして「システム情報」ウィンドウを開くことができます。
7. 「**ファイアウォール**」タブをクリックします。
8. デプロイメントの外部にあり、このホストに接続する必要があるデバイスのためのアクセスを構成します。
9. 矢印をクリックしてこのアクセス・ルールを追加します。
10. 「**保存**」をクリックします。

© Copyright IBM Corp. 2012, 2015

アラートと通知用の E メール・サーバーの追加

QRadar Risk Manager により使用されるメール・サーバーを構成できます。これは、アラートとイベント・メッセージを配布するために使用されます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**システム構成**」をクリックします。
3. 「**システムおよびライセンス管理**」アイコンをクリックします。
4. 「**表示**」メニューから、「**システム**」を選択します。
5. E メール・サーバー・アドレスを追加するホストを選択します。
6. 「**アクション**」メニューから、「**システムの表示と管理**」を選択します。

   注: ホストを右クリックして、このメニューにアクセスすることもできます。またはホストをダブルクリックして、「システム情報」ウィンドウを開くこともできます。
7. 「**E メール・サーバー**」タブをクリックします。
8. 「**E メール・サーバー・アドレス**」フィールドで、使用する E メール・サーバーのホスト名または IP アドレスを入力します。

   E メール・サーバーをポート 25 を使用して接続します。

   E メール・サーバーがなく、QRadar が提供する E メール・サーバーを使用する場合は、`localhost` と入力します。
9. 「**保存**」をクリックします。

ネットワーク・インターフェースの構成

QRadar Risk Manager のネットワーク・インターフェース用の IP アドレス情報およびロールを構成します。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**システム構成**」をクリックします。
3. 「**システムおよびライセンス管理**」アイコンをクリックします。
4. 「**表示**」メニューから、「**システム**」を選択します。
5. ネットワーク・インターフェース設定を編集するホストを選択します。
6. 「**アクション**」 > 「**システムの表示と管理**」をクリックするか、または選択したデバイスを右クリックしてこのメニュー・オプションにアクセスします。 ホストをダブルクリックして「システム情報」ウィンドウを開くこともできます。
7. 「**ネットワーク・インターフェース**」タブをクリックします。
8. 「**デバイス**」列からネットワーク・インターフェースを選択します。
9. 「**編集**」をクリックします。

管理、HA クロスオーバー、またはスレーブのロールを持つネットワーク・インターフェースは編集できません。

10. 以下のパラメーターを構成します。
    - 「**ロール**」。
    - IP アドレス属性。
    - 「**アクティブ HA を備えたこの構成を移動**」オプション。
11. 「**保存**」をクリックして設定を更新します。

ルート・パスワードの変更

定期的、または少なくとも 90 日ごとに IBM Security QRadar Risk Manager ホストの root パスワードを変更できます。

手順

1. SSH を使用して、root ユーザーとして QRadar コンソールにログインします。
2. root ユーザーのユーザー名およびパスワードを入力します。

   ユーザー名とパスワードは、大/小文字が区別されます。
3. QRadar コンソール から、SSH を使用して root ユーザーとして QRadar Risk Manager にログインします。
4. **passwd** コマンドを使用してパスワードを変更します。

   ルート・パスワードには、アポストロフィ (')、ドル記号 ($)、感嘆符 (!) を使用することはできません。

システム時刻の更新

すべてのシステム時刻の変更は、QRadar コンソールで設定する必要があります。QRadar コンソールで時刻同期サービスを有効にして、管理対象ホストと時刻を同期させます。

このタスクについて

コンソールでのシステム時刻の構成、およびデプロイメント環境での管理対象ホストとの時刻の同期について詳しくは、「IBM Security QRadar SIEM 管理ガイド」を参照してください。

手順

1. SSH を使用して、root ユーザーとして QRadar コンソールにログインします。
2. ntp.conf ファイルを編集します。

   ```
   vi /etc/ntp.conf
   ```
3. ntp.conf ファイルの *server* セクションでは、既存のサーバー項目をそのままにしておくことも、独自の内部 NTP (Network Time Protocol) サーバーと置き換えることもできます。 ntp.conf ファイル内のサーバー項目は、「server」で始まります。

   NTP プロジェクト (http://www.ntp.org/) の公開サーバーを使用できます。

```
server 0.rhel.pool.ntp.org iburst
server 1.rhel.pool.ntp.org iburst
server 2.rhel.pool.ntp.org iburst
server 3.rhel.pool.ntp.org iburst
```

公開 NTP サーバーを使用する場合、ファイアウォールがアウトバウンド NTP 要求を許可していることを確認します。

4. 変更内容を保存し、ファイルを閉じます。
5. ntpd サービスを、実行レベル 3 で実行できるようにします。

   ```
   chkconfig --level 3 ntpd on
   ```

6. 再始動時に ntpd サービスが実行可能になっていることを確認します。

   ```
   chkconfig --list ntpd
   ```

   出力に 3:on が表示されていることを確認します。これにより、サービスが有効になっていることが確認されます。

   ```
   ntpd 0:off 1:off 2:off 3:on 4:off 5:off 6:off
   ```

   NTP サーバーと時刻を手動で同期するには、サービスをシャットダウンする必要があります。

7. システム時刻の変更時のデータ収集エラーを防ぐために、QRadar サービスをシャットダウンします。

   ```
   service hostcontext stop

   service tomcat stop

   service hostservices stop
   ```

8. NTP サーバーと時刻を同期します。

   ```
   ntpdate <ntp.server.address>
   ```

9. ntpd サービスを始動します。

   ```
   service ntpd start
   ```

10. QRadar サービスを再始動します。

    ```
    service hostservices start

    service tomcat start

    service hostcontext start
    ```

11. 次のコマンドを入力して、すべての管理対象ホストの時刻を QRadar コンソールと同期します。

    ```
    /opt/qradar/support/all_servers.sh /opt/qradar/bin/time_sync.sh
    ```

12. 「**管理**」タブから、「**拡張**」 > 「**すべての構成のデプロイ**」をクリックして、すべての QRadar 管理対象ホストのサービスを再始動します。

    これで QRadar コンソールと管理対象ホストとの間で時刻が同期しました。

第 4 章 構成ソース管理

IBM Security QRadar Risk Manager で、資格情報の構成、デバイスの追加またはディスカバー、デバイス構成の表示、およびデバイス構成のバックアップを行う際に、構成ソース管理を使用します。

ネットワーク内のデバイスから取得されたデータを使用して、トポロジーにデータが取り込まれます。IBM Security QRadar SIEM の「**管理**」タブから構成ソース管理機能にアクセスするには、管理特権が必要です。

構成ソースをセットアップするには、以下を実行する必要があります。

1. デバイス資格情報を構成します。
2. デバイスをディスカバーまたはインポートします。ネットワーク・デバイスを QRadar Risk Manager に追加する 2 つの方法として、構成ソース管理を使用してデバイスをディスカバーするか、デバイス・インポートを使用して CSV ファイルからデバイスのリストをインポートします。
3. すべてのデバイスからデバイス構成を取得します。
4. デバイス構成のすべての更新が取り込まれるようにバックアップ・ジョブを管理します。
5. 新しいデバイスが自動的にディスカバーされるようにディスカバリー・スケジュールをセットアップします。

構成ソース管理は、以下の目的で使用します。

- 構成ソースを追加、編集、検索、および削除する。詳しくは、デバイスの管理を参照してください。
- デバイスの通信プロトコルを構成または管理する。詳しくは、プロトコルの構成を参照してください。

Juniper NSM デバイスを使用している場合は、さらに構成情報を取得する必要があります。

特定の製造元のデバイスと通信するために使用するアダプターについて詳しくは、「*IBM Security QRadar Risk Manager Adapter Configuration Guide*」を参照してください。

資格情報

IBM Security QRadar Risk Manager では、ファイアウォール、ルーター、スイッチ、IPS などのデバイスの構成にアクセスしてダウンロードする際に資格情報を使用します。

管理者は、構成ソース管理を使用して、デバイス資格情報を入力します。これにより、特定のデバイスに対する QRadar Risk Manager アクセス権限が付与されます。特定のネットワーク・デバイスに対し、個別のデバイス資格情報を保存できます。複数のネットワーク・デバイスが同じ資格情報を使用する場合は、資格情報をグループに割り当てることができます。

© Copyright IBM Corp. 2012, 2015

例えば、組織内のすべてのファイアウォールが同じユーザー名とパスワードを使用している場合、資格情報をそれらのすべてのファイアウォールのアドレス・セットに関連付けて、組織内のすべてのファイアウォールのデバイス構成をバックアップするために使用します。

特定のデバイスでネットワーク資格情報が不要な場合、構成ソース管理内の資格情報のパラメーターを空白のままにできます。必須のアダプター資格情報のリストについては、「*IBM Security QRadar Risk Manager Adapter Configuration Guide*」を参照してください。

ネットワーク内のさまざまなデバイスをネットワーク・グループに割り当てることで、デバイスの資格情報セットとアドレス・セットをグループ化することができます。

資格情報セット

資格情報セットには、一連のデバイスのユーザー名およびパスワードの値などの情報が含まれます。

ネットワーク・グループ

ネットワーク・グループごとに、複数の資格情報セットとアドレス・セットを含めることができます。各ネットワーク・グループの評価方法に優先順位を付けるように IBM Security QRadar Risk Manager を構成できます。

リストの先頭にあるネットワーク・グループに、最も高い優先順位が付けられます。構成済み IP アドレスと一致する最初のネットワーク・グループが、デバイス・バックアップ時の候補として含められます。考慮されるネットワーク・グループの資格情報セットは、最大 3 つです。

例えば、構成に以下の 2 つのネットワークが含まれているとします。

- 2 つの資格情報セットが含まれるネットワーク・グループ 1
- 2 つの資格情報セットが含まれるネットワーク・グループ 2

QRadar Risk Manager は、最大 3 つの資格情報セットのリストをコンパイルしようと試みます。ネットワーク・グループ 1 はリストの上位に位置するため、ネットワーク・グループ 1 の資格情報セットはどちらも候補のリストに追加されます。3 つの資格情報セットが要求されるため、ネットワーク・グループ 2 の最初の資格情報セットがリストに追加されます。

資格情報セットでデバイスに正常にアクセスすると、QRadar Risk Manager はこの資格情報セットを使用して、以降のデバイスへのアクセスを試行します。デバイスの資格情報が変更された場合、そのデバイスへのアクセスを試行すると、認証に失敗します。この場合、次回の認証試行時に、QRadar Risk Manager は確実に成功するよう資格情報を再調整します。

アドレス・セット

アドレス・セットとは、同じ資格情報のセットを共有するデバイスのグループを定義する IP アドレスのリストです。

IBM Security QRadar Risk Manager の資格情報の構成

管理者は、IBM Security QRadar Risk Manager がネットワーク内のデバイスに接続できるようにするために資格情報を構成する必要があります。

このタスクについて

ダッシュまたはワイルドカード (*) を使用して IP アドレス範囲を入力することで範囲を示すことができます (10.100.20.0-10.100.20.240 や 1.1.1* など)。 1.1.1.* と入力すると、その要件を満たすすべての IP アドレスが含まれます。

Juniper Networks NSM や汎用 XML アダプターを使用してアドレス・セットを構成する場合、Juniper Networks NSM やリポジトリー内のデバイス用のファイルにより管理されるすべてのデバイスの IP アドレス範囲または CIDR アドレス範囲を入力する必要があります。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・ペインで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. ナビゲーション・メニューで「**資格情報 (Credentials)**」をクリックします。
5. 「**ネットワーク・グループ (Network Groups)**」ペインで、「**追加 (+)**」アイコンをクリックします。
6. ネットワーク・グループの名前を入力し、「**OK**」をクリックします。
7. 優先度を最も高くするネットワーク・グループをリストの先頭に移動します。「**上に移動**」と「**下に移動**」の矢印アイコンを使用してネットワーク・グループの優先順位付けを行えます。
8. 「**アドレスの追加 (Add Address)**」フィールドに、ネットワーク・グループに適用する IP アドレスまたは CIDR 範囲を入力して、「**追加 (+)**」アイコンをクリックします。

   このネットワーク・グループ用のアドレス・セットに追加するすべての IP アドレスについてこれを繰り返します。
9. 「**資格情報 (Credentials)**」ペインで、「**追加 (+)**」アイコンをクリックします。
10. 新規資格情報セットの名前を入力し、「**OK**」をクリックします。
11. 以下のパラメーターの値を入力します。

オプション	説明
ユーザー名	資格情報セットのユーザー名を入力します。 Juniper Networks NSM または汎用 XML アダプターを使用している場合、Juniper NSM サーバーにアクセス可能なユーザー名か、SED (標準エレメント文書) ファイルを含むファイル・リポジトリーにアクセス可能なユーザー名を入力します。
パスワード	資格情報セットのパスワードを入力します。 Juniper Networks NSM または汎用 XML アダプターを使用している場合、Juniper NSM サーバー用のパスワード、または SED (標準エレメント文書) ファイルを含むファイル・リポジトリーにログインするためのパスワードを入力します。
ユーザー名を有効にする (Enable Username)	資格情報セットの第 2 レベル認証用のユーザー名を入力します。
パスワードを有効にする (Enable Password)	資格情報セットの第 2 レベル認証用のパスワードを入力します。
SNMP Get コミュニティー (SNMP Get Community)	SNMP Get コミュニティーを入力します。
SNMPv3 認証ユーザー名 (SNMPv3 Authentication Username)	SNMPv3 の認証に使用するユーザー名を入力します。
SNMPv3 認証パスワード (SNMPv3 Authentication Password)	SNMPv3 の認証に使用するパスワードを入力します。
SNMPv3 プライバシー・パスワード (SNMPv3 Privacy Password)	SNMPv3 トラップの復号に使用するプロトコルを入力します。

12. 優先度を最も高くする資格情報セットをリストの先頭に移動します。「**上に移動**」と「**下に移動**」の矢印アイコンを使用して資格情報セットの優先順位付けを行います。
13. 追加する資格情報セットごとに繰り返します。
14. 「**OK**」をクリックします。

デバイスのディスカバリー

ディスカバリー・プロセスでは、Simple Network Management Protocol (SNMP) とコマンド・ライン (CLI) を使用してネットワーク・デバイスをディスカバーします。

IP アドレスまたは CIDR 範囲を構成すると、ポート 22、23、または 443 で接続をモニターしているかどうかを判別するために、ディスカバリー・エンジンがその IP アドレスに対して TCP スキャンを実行します。TCP スキャンが正常に行われ、デバイスのタイプを判別するための SNMP 照会が構成されるときに、IP アドレスに基づいて SNMP GET コミュニティー・ストリングが使用されます。

この情報は、デバイスの追加時にそのマップ先となるアダプターを決定するために使用されます。IBM Security QRadar Risk Manager はデバイスに接続し、CDP、NDP、ARP の各テーブルなど、インターフェースと近隣情報のリストを収集します。その上で、デバイスがインベントリーに追加されます。

ディスカバリー・プロセスを開始する際に使用するよう構成した IP アドレスは、新しいデバイスに割り当てられる IP アドレスではない場合があります。QRadar Risk Manager は、デバイスで最小番号が付けられたインターフェースの IP アドレス (または最小のループバック・アドレスがある場合はそのアドレス) を使用してデバイスを追加します。

「**上記で定義したアドレスからネットワークをクロール (Crawl the network from the addresses defined above)**」チェック・ボックスを使用すると、デバイスから収集された近隣の IP アドレスがディスカバリー・プロセスに再び取り込まれ、IP アドレスごとにプロセスが繰り返されます。

デバイスのディスカバー

管理者は「デバイスのディスカバー (Discover Devices)」を使用してデバイスのタイプを判別します。

このタスクについて

デバイス・ディスカバリーを実行する際に、サポート対象ではないが SNMP に応答するデバイスは、汎用 SNMP アダプターを使用して追加されます。そのデバイスを通るパス・フィルターをシミュレート・ルートにより実行する場合は、そのデバイスを手動で削除する必要があります。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. ナビゲーション・メニューで、「**デバイスのディスカバー (Discover Devices)**」をクリックします。
5. IP アドレスまたは CIDR 範囲を入力します。

   この IP アドレスまたは CIDR範囲 は、ディスカバーするデバイスのロケーションを示します。
6. 「**追加 (+)**」アイコンをクリックします。
7. 定義した IP アドレスまたは CIDR 範囲からもネットワーク内のデバイスの検索を実行する場合は、「**上記で定義したアドレスからネットワークをクロール (Crawl the network from the addresses defined above)**」チェック・ボックスを選択します。
8. 「**実行**」をクリックします。

デバイスのインポート

コンマ区切り値ファイル (.CSV) を使用して、アダプターとそのネットワーク IP アドレスのリストを構成ソース管理に追加する際に、デバイス・インポートを使用します。

デバイス・インポート・リストには最大 5000 のデバイスを含めることができます。ただし、インポート・ファイル内のこのリストでは、各アダプターおよびその関連付けられた IP アドレスに対して 1 行ずつ含めなければなりません。

例えば、以下のようにします。

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

各部分について以下で説明します。

<Adapter::Name> には、製造元とデバイス名が含まれます (例: Cisco::IOS)。

<IP Address> には、デバイスの IP アドレスが含まれます (例: 191.168.1.1)。

表 3. デバイス・インポートの例

製造元	名前	例 <Adapter::Name>,<IP Address>
Check Point	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Cisco Security Appliance	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Cisco	Nexus	Cisco::Nexus
汎用	SNMP	Generic::SNMP,10.1.1.8
Juniper Networks	Junos	Juniper::JUNOS,10.1.1.5

CSV ファイルのインポート

コンマ区切り値 (CSV) ファイルを使用して、マスター・デバイス・リストを「構成ソース管理 (Configuration Source Management)」にインポートできます。

始める前に

デバイスのリストをインポートし、CSV ファイルで IP アドレスに変更を加えると、「構成ソース管理 (Configuration Source Management)」リスト内でデバイスが誤って重複してしまう可能性があります。この理由から、マスター・デバイス・リストを再インポートする前に、「構成ソース管理 (Configuration Source Management)」からデバイスを削除してください。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**プラグイン**」ペインで、「**デバイス・インポート**」をクリックします。

4. 「**表示 (Browse)**」をクリックします。
5. CSV ファイルを見つけて、「**オープン**」をクリックします。
6. 「**デバイスのインポート (Import Devices)**」をクリックします。

タスクの結果

エラーが表示された場合は、CSV ファイルを確認してエラーを訂正し、そのファイルを再インポートする必要があります。 CSV ファイルのインポートは、デバイス・リストの構造が誤っているか、またはデバイス・リストに誤った情報が含まれている場合に失敗する可能性があります。例えば、CSV ファイルにコロンまたはコマンドがない、複数のデバイスが単一行に記載されている、またはアダプター名にタイプミスがある、などの可能性があります。

デバイスのインポートが異常終了した場合は、CSV ファイルから「構成ソース管理 (Configuration Source Management)」にデバイスは追加されません。

デバイスの管理

「構成ソース管理」ウィンドウの「デバイス」タブを使用して、ネットワーク内のデバイスを管理できます。

「デバイス」タブで、デバイスを表示、追加、編集、および削除できます。また、デバイス・リストのフィルタリング、デバイス構成情報の取得、隣接データの収集、およびデプロイメント環境内のデバイスのディスカバーを行うこともできます。

デバイスの表示

「**デバイス**」タブでデプロイメント内のすべてのデバイスを表示できます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. 「**デバイス**」タブをクリックします。
5. デバイス構成の詳細情報を表示するには、表示するデバイスを選択し、「**オープン**」をクリックします。

デバイスの追加

構成ソース管理を使用して個々のネットワーク・デバイスおよびアダプターを追加することができます。

このタスクについて

構成ソース管理で個別のデバイスをデバイス・リストに追加することも、CSV ファイルを使用して複数のデバイスを追加することもできます。

複数のデバイスの追加について詳しくは、デバイスのインポートを参照してください。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. ナビゲーション・ペインで「**デバイスの追加 (Add Device)**」をクリックします。
5. 次の各パラメーターの値を構成します。

オプション	説明
IP アドレス	デバイスの管理 IP アドレスを入力します。
アダプター (Adapter)	「**アダプター (Adapter)**」ドロップダウン・リストから、このデバイスに割り当てるアダプターを選択します。

6. 「**追加**」をクリックします。

   必要な場合は、「**実行**」をクリックしてアダプター・リストを最新表示します。

デバイスの編集

エラーが発生した場合、またはネットワークが変更されて IP アドレスを再割り当てする必要がある場合に、デバイスを編集して IP アドレスまたはアダプター・タイプを修正できます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. 編集するデバイスを選択します。
5. 「**編集**」をクリックします。
6. 次の各パラメーターの値を構成します。

オプション	説明
IP アドレス	デバイスの管理 IP アドレスを入力します。
アダプター (Adapter)	「**アダプター (Adapter)**」ドロップダウン・リストから、このデバイスに割り当てるアダプターを選択します。

7. 「**保存**」をクリックします。

デバイスの削除

IBM Security QRadar Risk Manager からデバイスを削除できます。削除されたデバイスは、構成ソース管理 (Configuration Source Management)、構成モニター (Configuration Monitor)、およびトポロジーから削除されます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. 「**デバイス**」タブをクリックします。
5. 削除したいデバイスを選択します。
6. 「**削除**」をクリックします。
7. 「**はい**」をクリックしてデバイスを削除します。

タスクの結果

デバイスを削除した後、トポロジーからデバイスを削除する処理に数分かかる場合があります。

デバイス・リストのフィルタリング

フィルターを使用して、デバイス・リスト中のデバイスを迅速に見つけることができます。

このタスクについて

IBM Security QRadar Risk Manager は、「構成ソース管理 (Configuration Source Management)」で、最大 5000 のネットワーク・デバイスを処理できます。多数のネットワーク・デバイスがあると、デバイス・リスト全体のスクロールに手間がかかる場合があります。

以下の表は、デバイスをさらに迅速に見つけるために、デバイス・リストに適用できるフィルターのタイプを説明しています。

表 4. デバイス・リストのフィルター・タイプ

検索オプション	説明
インターフェース IP アドレス	IP アドレスまたは CIDR 範囲のいずれかと一致するインターフェースを持つデバイスをフィルターで検出します。 「IP/CIDR」フィールドに、検索する IP アドレスまたは CIDR 範囲を入力します。 例えば、10.100.22.6 という検索条件を入力すると、検索結果では 10.100.22.6 という IP アドレスを持つデバイスが返されます。10.100.22.0/24 という CIDR 範囲を入力すると、10.100.22.* のすべてのデバイスが返されます。
管理 IP アドレス	管理インターフェース IP アドレスに基づいてデバイス・リストをフィルタリングします。管理 IP アドレスは、デバイスを一意に識別する IP アドレスです。 「**IP/CIDR**」フィールドに、検索する IP アドレスまたは CIDR 範囲を入力します。
OS バージョン	デバイスが実行されているオペレーティング・システムのバージョンに基づいてデバイス・リストをフィルタリングします。 次の各パラメーターの値を選択します。 • 「**アダプター**」 - このドロップダウン・リストを使用して、検索するアダプターのタイプを選択します。 • 「**バージョン**」 - このドロップダウン・リストを使用して、バージョンの検索条件を選択します。例えば、指定値に対して「より大」、「より小」、「次に等しい」を指定します。フィールドに検索対象のバージョン番号を入力します。バージョンの検索オプションを選択しない場合、結果には、バージョンに関係なく、選択されたアダプターで構成されているすべてのデバイスが含まれます。
モデル	ベンダーとモデル番号に基づいてデバイス・リストをフィルタリングします。 次の各パラメーターの値を構成します。 • 「**ベンダー**」 - このドロップダウン・リストを使用して、検索するベンダーを選択します。 • 「**モデル**」 - 検索するモデルを入力します。

表 4. デバイス・リストのフィルター・タイプ (続き)

検索オプション	説明
ホスト名	ホスト名に基づいてデバイス・リストをフィルタリングします。 「**ホスト名**」フィールドに、検索対象のホスト名を入力します。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「Risk Manager」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. 「**デバイス**」タブをクリックします。
5. デバイス・リストの左側にあるドロップダウン・リストを使用して、フィルターを選択します。
6. 「**実行**」をクリックします。

タスクの結果

条件に一致するすべての検索結果が表に表示されます。

次のタスク

フィルターをリセットするには、「**インターフェース IP アドレス (Interface IP Address)**」を選択し、「**IP/CIDR**」のアドレスをクリアしてから、「**実行**」をクリックします。

デバイス構成の取得

デバイス構成を取得するためにデバイスをバックアップするプロセスは、デバイス・リスト内の単一デバイスに対して実行できます。または「**デバイス**」タブにあるすべてのデバイスをバックアップすることもできます。

このタスクについて

ネットワーク・デバイスにアクセスするために資格情報セットとアドレス・セットを構成した後に、デバイス情報がトポロジーに含まれるように、デバイスをバックアップしてデバイス構成をダウンロードする必要があります。

「**ジョブ**」タブからデバイス構成の自動バックアップをスケジュールする方法について詳しくは、『バックアップ・ジョブの管理』を参照してください。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。

4. 「**デバイス**」タブをクリックします。
5. すべてのデバイスの構成を取得するには、ナビゲーション・ペインで「**すべてをバックアップ (Backup All)**」をクリックし、「**はい**」をクリックして先に進みます。
6. 1 つのデバイスの構成を取得するには、そのデバイスを選択します。複数のデバイスを選択するには、CTRL キーを押したまま、必要なデバイスをすべて選択します。「**バックアップ**」をクリックします。
7. 必要な場合は、「**エラーの表示 (View Error)**」をクリックして、エラーの詳細を表示します。エラーを訂正した後に、ナビゲーション・ペインで「**すべてをバックアップ (Backup All)**」をクリックします。

近隣データの収集

SNMP およびコマンド・ライン・インターフェース (CLI) を使用してデバイスから近隣データを取得するには、ディスカバリー処理を使用します。

このタスクについて

トポロジーで接続線を描き、ネットワーク・デバイスのグラフィカルなトポロジー・マップを表示するために、近隣データが使用されます。「ディスカバー (discover)」ボタンにより、単一または複数のデバイスを選択してデバイスの近隣データを更新することができます。この情報は、トポロジーの 1 つ以上のデバイスの接続線を更新するために使用されます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. 「**デバイス**」タブをクリックします。
5. データを取得するデバイスを選択します。複数のデバイスを選択するには、CTRL キーを押したまま、必要なデバイスをすべて選択します。
6. 「**ディスカバー (Discover)**」をクリックします。
7. 「**はい**」をクリックして先に進みます。

タスクの結果

複数のデバイスを選択した場合は、ディスカバー処理が完了するまで数分かかることがあります。

次のタスク

他の作業を行うには、「**バックグラウンドで実行 (Run in Background)**」を選択します。

ファイル・リポジトリーからのデータ収集

ネットワーク・ファイル・リポジトリーから、基本的なデバイス構成を含むデバイス XML SED (標準エレメント文書) ファイルまたは入力ファイルを取得できます。

このタスクについて

ファイルをホストするファイル・リポジトリーは、FTP プロトコルまたは SFTP プロトコルをサポートする必要があります。IBM Security QRadar Risk Manager は、ファイル・リポジトリーのリモート・ファイル・ディレクトリーにあるすべての SED (標準エレメント文書) XML ファイルからデバイス情報を取得します。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. 「**デバイス**」タブをクリックします。
5. 「**リポジトリーからディスカバー (Discover from Repository)**」を選択します。
6. 次の各パラメーターの値を構成します。

オプション	説明
プロトコル	「**プロトコル**」ドロップダウン・リストから、構成ファイル・リポジトリーにアクセスするための通信プロトコルとして「**FTP**」または「**SFTP**」を選択します。
IP アドレス	構成ファイル・リポジトリーの IP アドレスを入力します。
リモート・パス (Remote Path)	SED (標準エレメント文書) XML ファイルを含むディレクトリーのリモート・ファイル・パスを入力します。SED (標準エレメント文書) ファイルのデフォルト・ファイル・パスは `<インストール・ディレクトリー>/output` です。`<インストール・ディレクトリー>` は、解凍した `ziptie-adapter.<date>-<build>.zip` ファイルの場所です。
ユーザー名	構成ファイル・リポジトリーをホストするシステムにログインするためのユーザー名を入力します。
パスワード	構成ファイル・リポジトリーをホストするシステムにログインするためのパスワードを入力します。

7. 「**OK**」をクリックして、リポジトリーからデバイスをディスカバーします。
8. 「**実行**」をクリックすると、デバイス・リストが最新表示されます。

バックアップ・ジョブの管理

ジョブがバックアップ・ジョブを参照することにより、スケジュールに従って、「**デバイス**」タブ内のすべてのデバイスの構成情報を自動的にバックアップすることができます。

「構成ソース管理」の「**ジョブ**」タブを使用して、すべてのデバイスまたはデバイスの個々のグループに対するバックアップ・ジョブを構成ソース管理で作成できます。

「構成ソース管理」ページで定義するバックアップ・ジョブはどれも、「**管理**」タブの「**バックアップおよびリカバリー**」アイコンを使用する IBM Security QRadar SIEM バックアップ構成には影響を与えません。バックアップおよびリカバリー機能は、QRadar SIEM の構成情報とデータを取得します。バックアップ・ジョブが取得するのは、外部デバイスの情報のみです。

バックアップ・ジョブの表示

ジョブおよびジョブの詳細は、「**ジョブ**」タブに表示されます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. 「**ジョブ**」タブをクリックします。
5. さらに詳細に表示するジョブをダブルクリックします。

バックアップ・ジョブの状況とログの表示

バックアップ・ジョブに関する問題のトラブルシューティングを行うには、「**構成モニター (Configuration Monitor)**」ページに表示されるバックアップの状況とログ・ファイルに関する情報を使用します。

このタスクについて

バックアップ・ジョブの処理状況と進行状況を表示するには、「構成モニター (Configuration Monitor)」ページを使用します。バックアップ・ジョブのログ・ファイルを表示するには、バックアップ・ログ・ビューアーを使用します。

手順

「**リスク**」 > 「**構成モニター (Configuration Monitor)**」に移動します。以下に示す「**デバイス・リスト**」表の各列に、バックアップ・ジョブの状況に関する情報が表示されます。

列	説明
バックアップの状況 (Backup Status)	バックアップ・ジョブの実行状況を示します。 • 収集 (COLLECTED): バックアップ・ジョブは処理待ちの状態です。 • 実行中 (RUNNING): バックアップ・ジョブは実行中です。 • 成功 (SUCCESS): バックアップ・ジョブは正しく実行されました。 • 失敗 (FAILURE): バックアップ・ジョブは完了しませんでした。
進行	バックアップ・ジョブの完了率を示す進行状況表示バーが表示されます。 この進行状況表示バーを更新するには、「構成モニター (Configuration Monitor)」ページの「**最新表示**」アイコンをクリックします。
バックアップ・ログ (Backup Log)	バックアップ・ジョブの「バックアップ・ログ・ビューアー (Backup Log Viewer)」ウィンドウを開くには、この列の「**ログの表示 (See Log)**」リンクをクリックします。 進行状況表示バーを更新するには、「バックアップ・ログ・ビューアー (Backup Log Viewer)」ウィンドウの「**再表示**」をクリックします。

バックアップ・ジョブの追加

構成ソース管理では、すべてのデバイスまたは個々のデバイス・グループのバックアップ・ジョブを作成できます。

このタスクについて

検索条件を定義した後は、ジョブ・スケジュールを定義します。スケジュール構成が「トリガー (Triggers)」列に表示されます。ジョブのトリガーはジョブ・スケジュールを表します。複数のスケジュールを構成することができます。例えば、スケジュール・オプションを 2 つ構成して、ジョブを毎週月曜日と毎月 1 日に実行することができます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. 「**ジョブ**」タブをクリックします。
5. 「**新規ジョブ (New Job)**」 > 「**バックアップ**」を選択します。
6. 次の各パラメーターの値を構成します。

オプション	説明
ジョブ名	このジョブに適用する名前を入力します。

オプション	説明
グループ	「グループ」リストから、このジョブを割り当てるグループを選択します。 グループがリストされない場合は、グループ名を入力できます。ジョブをグループに割り当てると、ジョブをソートできます。
コメント	このバックアップ・ジョブに関連付ける任意のコメントを入力します。バックアップ・ジョブの説明には 255 文字まで入力できます。

7. 「**OK**」をクリックします。
8. 以下のいずれかの検索方法を選択します。

オプション	説明
静的リスト (Static list)	いくつかのオプションを使用することで、静的リストを使用してデバイスを検索することができます。静的リスト・オプションを使用して、ジョブを実行する特定のデバイスを定義することができます。
検索	ジョブに含める IP アドレスまたは CIDR 範囲を入力します。検索条件を定義すると、ジョブの実行後にデバイスが検索されます。これにより、すべての新規デバイスがジョブに含まれるようになります。

9. 静的リストを選択した場合は、以下のようにして検索条件を定義します。
   a. 「**デバイス**」タブをクリックします。
   b. 「**デバイス**」タブ上のリストから、検索条件を選択します。詳しくは、静的リストまたは検索の検索条件を参照してください。
   c. 「**実行**」をクリックします。
   d. 「**デバイス**」タブで、ジョブに含めるデバイスを選択します。
   e. 「ジョブの詳細 (Job Details)」ペインで、「**デバイス・ビュー検索から選択した項目を追加 (Add selected from device view search)**」をクリックします。
10. 「検索」を選択した場合は、以下のようにして検索条件を定義します。
    a. 「**デバイス**」タブをクリックします。
    b. 「**デバイス**」タブのリストを使用して、検索条件を選択します。詳しくは、静的リストまたは検索の検索条件を参照してください。
    c. 「**実行**」をクリックします。
    d. 「ジョブの詳細 (Job Details)」ペインで、「**デバイス・ビューからの検索を使用 (Use search from devices view)**」をクリックします。この検索条件を使用して、このジョブに関連付けられるデバイスが判別されます。
11. 「**スケジュール**」をクリックし、以下のパラメーターの値を構成します。

オプション	説明
名前	スケジュール構成の名前を入力します。
開始時刻	バックアップ処理を開始する時刻と日付を選択します。時刻は 24 時間表記で指定する必要があります。
頻度	このスケジュールに関連付ける頻度を選択します。
Cron	グリニッジ標準時 (GMT) で解釈される、クーロン式を入力します。詳しくは、管理者にお問い合わせください。
終了日の指定 (Specify End Date)	オプション。ジョブ・スケジュールを終了する日付を選択します。

12. 「トリガー (Trigger)」ペインの「**保存**」をクリックします。
13. 複数のスケジュールを作成するには、ステップ 11 および 12 を繰り返します。
14. ジョブを直ちに実行する場合は、「**今すぐ実行**」をクリックします。
15. 「**はい**」をクリックして先に進みます。

バックアップ・ジョブの編集

バックアップ・ジョブを編集することができます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. 「**ジョブ**」タブをクリックします。
5. 編集するジョブをダブルクリックします。
6. 「**選択タイプ (Selection Type)**」パラメーターで以下の検索オプションのいずれかを選択します。

オプション	説明
静的リスト (Static list)	静的リストを使用すると、複数のオプションを使用してデバイスを検索することができます。静的リスト・オプションを使用して、ジョブを実行する特定のデバイスを定義することができます。
検索	ジョブに含める IP アドレスまたは CIDR 範囲を入力します。検索条件を定義すると、デバイスの検索はジョブの実行後に発生します。これにより、すべての新規デバイスがジョブに含まれるようになります。

7. 静的リストを選択した場合は、以下のようにして検索条件を定義します。

a. 「**デバイス**」タブをクリックします。
b. 「**デバイス**」タブ上のリストから、検索条件を選択します。
c. 「**実行**」をクリックします。
d. 「**デバイス**」タブから、ジョブに含めるデバイスを選択します。
e. 「**ジョブの詳細 (Job Details)**」ペインで、「**デバイス・ビュー検索の選択項目の追加 (Add selected from device view search)**」をクリックします。

8. 「検索」を選択した場合、以下のようにして条件を定義します。
   a. 「**デバイス**」タブをクリックします。
   b. 「**デバイス**」タブのリストを使用して、検索条件を選択します。
   c. 「**実行**」をクリックします。
   d. 「ジョブの詳細 (Job Details)」ペインで、「**デバイス・ビューの検索を使用 (Use search from devices view)**」をクリックします。この検索条件を使用して、このジョブに関連付けられるデバイスが判別されます。
9. 「**スケジュール**」をクリックし、以下のパラメーターの値を構成します。

オプション	説明
名前	スケジュール構成の名前を入力します。
開始時刻	バックアップ処理を開始する時刻と日付を選択します。時刻は 24 時間表記で指定する必要があります。
頻度	このスケジュールに関連付ける頻度を選択します。
Cron	グリニッジ標準時 (GMT) で解釈される、クーロン式を入力します。詳しくは、管理者にお問い合わせください。
終了日の指定 (Specify End Date)	オプション。ジョブ・スケジュールを終了する日付を選択します。

10. 「**保存**」をクリックします。
11. 「**今すぐ実行**」をクリックします。
12. 必要に応じてステップ 9 と 10 を繰り返します。
13. 「**はい**」をクリックして先に進みます。

バックアップ・ジョブの名前変更

バックアップ・ジョブを名前変更できます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. 「**ジョブ**」タブをクリックします。
5. 名前変更するバックアップ・ジョブを選択します。

6. 「**名前変更**」をクリックします。
7. 次の各パラメーターの値を構成します。

オプション	説明
ジョブ名	このジョブに適用する名前を入力します。
グループ	「**グループ**」リストから、このジョブを割り当てるグループを選択します。新規グループ名を指定することもできます。
コメント	オプション。このバックアップ・ジョブに関連付ける任意のコメントを入力します。バックアップ・ジョブの説明には 255 文字まで入力できます。

8. 「**OK**」をクリックします。

バックアップ・ジョブの削除

バックアップ・ジョブを削除することができます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. 「**ジョブ**」タブをクリックします。
5. 削除するバックアップ・ジョブを選択します。
6. 「**削除**」をクリックします。

プロトコルの構成

IBM Security QRadar Risk Manager がデバイスと通信できるようにするために、ネットワーク・デバイスとの通信のために必要な通信方式 (プロトコル) を定義する必要があります。

QRadar Risk Manager には、使用するシステム用のデフォルト・プロトコル構成が用意されています。プロトコルを定義する必要がある場合、QRadar Risk Manager がデバイス構成の取得および更新を行えるようにするためのプロトコルを定義できます。多くのネットワーク環境で、デバイスのさまざまなタイプや機能のための各種通信プロトコルがあります。例えば、ルーターは、ネットワーク内のファイアウォールとは異なるプロトコルを使用する場合があります。デバイスの製造メーカーによりサポートされるプロトコルのリストについては、「*IBM Security QRadar Risk Manager Adapter Configuration Guide*」を参照してください。

QRadar Risk Manager では、プロトコル・セットを使用して、特定の通信プロトコルを必要とするデバイス・セット用のプロトコルのグループを定義します。デバイスをネットワーク・グループに割り当てることで、デバイスのプロトコル・セットとアドレス・セットをまとめることができます。

プロトコル・セットとは、特定のプロトコル資格情報を必要とするデバイス・セットのための名前が付けられたプロトコルのセットです。

アドレス・セットとは、ネットワーク・グループを定義する複数の IP アドレスのことです。

プロトコルの構成

デバイス構成を取得および更新するためのプロトコルを定義できます。

このタスクについて

プロトコル・パラメーターの以下の値を構成できます。

表 5. プロトコル・パラメーター

プロトコル	パラメーター
SSH	以下のパラメーターを構成します。 • **ポート** - ネットワーク・デバイスとの通信およびネットワーク・デバイスのバックアップで SSH プロトコルにより使用するポートを入力します。 デフォルトの SSH プロトコル・ポートは 22 です。 • **バージョン** - このネットワーク・グループでネットワーク・デバイスとの通信に使用する SSH のバージョンを選択します。選択可能なオプションは以下のとおりです。 **自動 (Auto)** - このオプションでは、ネットワーク・デバイスと通信する際に使用する SSH バージョンを自動的に検出します。 **1** - ネットワーク・デバイスと通信する際に SSH-1 を使用します。 **2** - ネットワーク・デバイスと通信する際に SSH-2 を使用します。
Telnet	ネットワーク・デバイスとの通信およびネットワーク・デバイスのバックアップで Telnet プロトコルにより使用するポート番号を入力します。 デフォルトの Telnet プロトコル・ポートは 23 です。
HTTPS	ネットワーク・デバイスとの通信およびネットワーク・デバイスのバックアップで HTTPS プロトコルにより使用するポート番号を入力します。 デフォルトの HTTPS プロトコル・ポートは 443 です。

表 5. プロトコル・パラメーター (続き)

プロトコル	パラメーター
HTTP	ネットワーク・デバイスとの通信およびネットワーク・デバイスのバックアップで HTTP プロトコルにより使用するポート番号を入力します。 デフォルトの HTTP プロトコル・ポートは 80 です。
SCP	ネットワーク・デバイスとの通信およびネットワーク・デバイスのバックアップで SCP プロトコルにより使用するポート番号を入力します。 デフォルトの SCP プロトコル・ポートは 22 です。
SFTP	ネットワーク・デバイスとの通信およびネットワーク・デバイスのバックアップで SFTP プロトコルにより使用するポート番号を入力します。 デフォルトの SFTP プロトコル・ポートは 22 です。
FTP	ネットワーク・デバイスとの通信およびネットワーク・デバイスのバックアップで FTP プロトコルにより使用するポート番号を入力します。 デフォルトの SFTP プロトコル・ポートは 22 です。
TFTP	TFTP プロトコルには構成可能なオプションはありません。

表 5. プロトコル・パラメーター (続き)

プロトコル	パラメーター
SNMP	以下のパラメーターを構成します。 • **ポート** - ネットワーク・デバイスとの通信およびネットワーク・デバイスのバックアップで SNMP プロトコルにより使用するポート番号を入力します。 • **タイムアウト (ミリ秒) (Timeout(ms))** - 通信タイムアウトを判別するために使用する時間 (ミリ秒) を選択します。 • **再試行 (Retries)** - デバイスとの通信を再試行する回数を選択します。 • **バージョン** - 通信に使用する SNMP のバージョンを選択します。オプションは v1、v2、または v3 です。 • **V3 認証 (V3 Authentication)** - SNMP トラップの認証に使用するアルゴリズムを選択します。 • **V3 暗号化 (V3 Encryption)** - SNMP トラップの復号に使用するプロトコルを選択します。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. ナビゲーション・メニューで、「**プロトコル**」をクリックします。
5. 以下のようにして新規ネットワーク・グループを構成します。
   a. 「**ネットワーク・グループ (Network Groups)**」ペインで、「**追加 (+)**」アイコンをクリックします。
   b. ネットワーク・グループの名前を入力します。
   c. 「**OK**」をクリックします。
   d. 「**上に移動**」と「**下に移動**」のアイコンを使用してネットワーク・グループの優先順位付けを行います。優先度を最も高くするネットワーク・グループをリストの先頭に移動します。
6. 以下のようにしてアドレス・セットを構成します。
   a. 「**アドレスの追加 (Add Address)**」フィールドに、ネットワーク・グループに適用する IP アドレスまたは CIDR 範囲を入力して、「**追加 (+)**」アイコンをクリックします。例えば、ダッシュまたはワイルドカード (*) を使用して IP アドレス範囲を入力することで範囲を示します (10.100.20.0-10.100.20.240 や 1.1.1* など)。1.1.1.* と入力すると、その要件を満たすすべての IP アドレスが含まれます。
   b. このネットワーク・グループ用のアドレス・セットに追加するすべての IP アドレスについてこれを繰り返します。

7. 以下のようにしてプロトコル・セットを構成します。
   a. 「**ネットワーク・グループ (Network Groups)**」ペインで、プロトコルを構成するネットワーク・グループが選択されていることを確認します。
   b. 作成したネットワーク・グループに割り当てられた IP アドレスの範囲にプロトコルを適用するためのチェック・ボックスを選択します。チェック・ボックスの選択をクリアすると、ネットワーク・デバイスのバックアップを試行する際にそのプロトコルの通信オプションがオフになります。
   c. 選択したプロトコルごとに、パラメーターの値を構成します。
   d. 「**上に移動**」と「**下に移動**」のアイコンを使用してプロトコルの優先順位付けを行います。優先度を最も高くするプロトコルをリストの先頭に移動します。
8. 「**OK**」をクリックします。

ディスカバリー・スケジュールの構成

デバイスの ARP、MAC テーブル、および近隣情報にデータを取り込むためのディスカバリー・スケジュールを構成できます。このディスカバリー・スケジュールにより、新規デバイスを自動的にインベントリーに追加することもできます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**プラグイン**」をクリックします。
3. 「**Risk Manager**」ペインで、「**構成ソース管理 (Configuration Source Management)**」をクリックします。
4. ナビゲーション・メニューで、「**ディスカバリーのスケジュール (Schedule Discovery)**」をクリックします。
5. 「**定期的なディスカバリーを有効にする (Enable periodic discovery)**」チェック・ボックスを選択してスケジュール・ディスカバリーを有効にします。
6. 次の各パラメーターの値を構成します。

オプション	説明
名前	スケジュール構成の名前を入力します。
開始時刻	バックアップ処理を開始する時刻と日付を選択します。時刻は 24 時間表記で指定する必要があります。
頻度	このスケジュールに関連付ける頻度を選択します。
Cron	グリニッジ標準時 (GMT) で解釈される、クーロン式を入力します。詳しくは、管理者にお問い合わせください。
終了日の指定 (Specify End Date)	オプション。ジョブ・スケジュールを終了する日付を選択します。

オプション	説明
クロールして新規デバイスをディスカバー (Crawl and discover new devices)	ディスカバリー・プロセスで新規デバイスをディスカバーする場合はこのチェック・ボックスを選択します。インベントリーに新規デバイスを追加しない場合は、チェック・ボックスをクリアします。

7. 「**OK**」をクリックします。

第 5 章 ネットワーク・トポロジー・グラフ

IBM Security QRadar Risk Manager では、トポロジー・モデル・グラフを使用して、ネットワークの物理接続の表示、フィルター操作、および調査を行えます。

ネットワーク・トポロジー・グラフは、デバイス (ファイアウォール、ルーター、スイッチ、侵入防止システム (IPS) など) から取得した構成情報から生成されます。接続線にマウス・カーソルを合わせると、ネットワーク接続の情報が表示されます。トポロジーをフィルターに掛けるには、許可されるプロトコル、ポート、または脆弱性に対する潜在的な攻撃パスを探索します。デバイスまたはサブネットの間のトラフィック・フローを表示したり、デバイス・ルールを表示したりすることができます。

トポロジー・グラフを使用すると、以下の作業が可能です。

- 特定のネットワーク・パスおよびトラフィックの方向を視覚化して、脅威の拡張分析を行う。
- パッシブ IPS セキュリティー・マップをトポロジー・グラフに取り込む。
- デバイスをグループ化することで、ビューを整理して単純化する。
- デバイスをグループに追加したり、グループからデバイスを削除したりする。
- マウスを使用してグラフ内のアイコンを位置変更する。
- トポロジー・グラフのレイアウトを保存する。
- デバイスおよびグループを名前変更する。
- プロトコル、ポート、または脆弱性に基づいてネットワーク・トポロジーの検索フィルターを作成し、保存する。
- デバイスとサブネットの間の詳細な接続情報を表示する。
- トポロジー・ノード接続に関するデバイス・ルールを、許可されたポートおよびプロトコルとともに表示する。
- ネットワーク・アドレス変換 (NAT) デバイス、NAT インディケーター、および NAT マッピングについての情報を表示する。
- 複数のコンテキストを持つ仮想ネットワーク・セキュリティー・デバイスを表示する。

デバイス間の許可されているポートおよびプロトコルを検索して閲覧するときにトポロジー・グラフに表示される接続は、TCP、UDP、および ICMP プロトコルを使用する接続のみです。

トポロジー・グラフの検索

トポロジーの検索機能を使用して、ネットワーク・インフラストラクチャーの各種エレメントを表示し、調査します。

検索機能を使用してトポロジー・ビューをフィルターに掛けて、ネットワーク・パス、ホスト、サブネット、およびその他のネットワーク・エレメントに絞り込むこ

© Copyright IBM Corp. 2012, 2015

とができます。ポートまたはプロトコルのレベルまで検索を絞り込むことができます。例えば、許可されたプロトコルまたはポート上の潜在的な攻撃パスを検索できます。

デバイスおよびサブネットを右クリックすると、イベントを検索できます。あるいは、サブネットを右クリックすると、フローを検索できます。

「**検索**」メニューにアクセスするには、「**アクション**」をクリックします。「検索条件」ペインに、検索条件を入力します。使用できる検索オプションの一部は以下のとおりです。

ホストの検索

ある特定のホストを検索すると、そのホストと通信するすべてのデバイスが表示されます。ホストがデバイスのインターフェースと一致していないが、サブネットに含まれている場合は、そのサブネットおよびすべての接続デバイスが表示されます。

ネットワークの検索

単一の CIDR を検索します (例: `10.3.51.200/24`)。

複数の CIDR を検索する場合は、それらの CIDR が有効であり、コンマで区切られていることを確認します (例えば、`10.51.0.0/24,10.51.01/24`)。

パスの検索

パスを検索すると、トラフィックの方向、完全または部分的に許可されたプロトコル、およびデバイス・ルールが表示されます。ネットワーク間にポート接続が存在する場合、パスのサマリーに許可ポートが表示されます。

接続上の**赤い正方形**は、ネットワーク・トラフィックがブロックされていることを示している場合があります。ネットワーク・トラフィックがノード A からノード B へと移動している場合、ノード A とノード B との間の接続上の**赤い正方形**は、以下を示している可能性があります。

- ノード B 上のファイアウォール・ルールによってトラフィックがブロックされている。
- ノード B に、パケットを転送するためのルートがない。

赤の正方形の上にマウス・ポインターを移動すると、詳細な情報が表示されます。

トポロジーでパスを選択すると、アプリケーションを検索できます (アプリケーションの検索を参照)。NAT インディケーターは、塗りつぶされた**緑の点**です。これがトポロジー・グラフに表示されるのは、検索によって返されたパスに、送信元または宛先の変換が含まれる場合です。

「**アクション**」メニューから、「**検索**」メニューにアクセスできます。

アプリケーションの検索

アプリケーションの詳細を表示するには、「**リスク**」タブから、またはトポロジーでパスを選択して、IBM Security QRadar Risk Manager トポロジーからアプリケーションを検索します。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**トポロジー**」をクリックします。
3. 「**検索**」 > 「**新規検索**」をクリックします。
4. 「**パス**」オプションを選択します。
5. 「**アプリケーションの選択**」をクリックします。
6. 「**デバイス・アダプター (Device Adapter)**」ドロップダウン・メニューで、必要なデバイス・アダプター・タイプを選択します。
7. 「**アプリケーション名**」フィールドに、アプリケーションの記述子を入力します。
8. 「**検索**」をクリックします。
9. 「**検索結果**」フィールドで検索対象の各アプリケーションをクリックして、「**追加**」をクリックします。
10. 「**OK**」をクリックします。

脆弱性による検索

トポロジー・グラフに侵入防止システム (IPS) を配置してある場合は、「**検索**」メニューから脆弱性による検索を実行できます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**トポロジー**」をクリックします。
3. 「**検索**」 > 「**新規検索**」をクリックします。
4. 「**パス**」オプションを選択します。
5. 「**脆弱性の選択 (Select Vulnerability)**」をクリックします。
6. 「**検索条件**」メニューから脆弱性のカテゴリーを選択します。
7. 「**検索条件**」メニューの横にある「**フィールド**」に脆弱性の ID 番号を入力します。
8. 「**検索**」をクリックします。
9. 「**検索結果**」フィールドで検索対象の各脆弱性をクリックして、「**追加**」をクリックします。
10. 「**保存**」をクリックします。
11. 「**検索**」をクリックすると結果が表示されます。

脆弱性検索オプションが表示されない場合は、侵入防止システム (IPS) の追加を参照してください。

検索結果内の NAT インディケーター

NAT インディケーター (緑色の塗りつぶしドット) は、送信元または宛先の変換が含まれているパスを検索で検出した場合に、トポロジー・グラフに表示されます。

このタスクについて

NAT インディケーターは、パス・フィルターで指定された宛先 IP アドレスが最終宛先ではない可能性があることを示します。インディケーター上にマウス・ポインターを移動すると、変換に関する以下の情報が表示されます。

表 6. NAT インディケーターから入手できる情報

パラメーター	説明
送信元	変換済みの送信元 IP または CIDR。
送信元ポート	変換済みの送信元ポート (該当する場合)。
変換済みの送信元	送信元に適用された変換の結果。
変換済みのソース・ポート	送信元ポートに適用された変換の結果 (該当する場合)。
宛先	変換済みの宛先 IP または CIDR。
宛先ポート	変換済みの宛先ポート (該当する場合)。
変換済みの宛先	宛先に適用された変換の結果。
変換済みの宛先ポート	宛先ポートに適用された変換の結果 (該当する場合)。
フェーズ	変換が適用されたときのルーティング・フェーズ。変換は、ルーティング前またはルーティング後のいずれかで適用されます。

侵入防止システム (IPS) の追加

「**構成ソース管理 (Configuration Source Management)**」リストに侵入防止システム (IPS) デバイスが含まれている場合、デバイスからサブネットへのノードの間、およびデバイスからデバイスへのノードの間の接続に IPS を追加できます。

このタスクについて

IPS 接続を追加すると、デバイスがパッシブである場合の IPS ロケーションの判別に役立ちます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**トポロジー**」をクリックします。
3. デバイス・ノードとサブネット・ノードをつなぐ接続線にマウス・ポインターを移動します。
4. 接続線を右クリックして「**IPS の追加 (Add IPS)**」を選択します。
5. 追加するデバイスおよびインターフェースを以下のリストから選択します。

オプション	説明
IPS の配置 (Place IPS)	リストから配置を選択します。
IPS インターフェースの接続 (Connect IPS interface)	デバイスに接続するインターフェースを選択します。複数のデバイスから選択できる場合は、デバイスを選択する必要があります (次のオプションを参照してください)。
接続先デバイス (to device)	IPS に接続するデバイスを選択します。このオプションは、複数のデバイスがある場合に使用できます。
IPS インターフェースの接続 (Connect IPS interface)	サブネットに接続するインターフェースを選択します。

6. リストを使用して、IPS 接続をトポロジーに追加するデバイスおよびインターフェースを選択します。
7. 「**OK**」をクリックします。 グループ内のデバイスに IPS を追加する場合は、グループを展開して IPS を追加します。

侵入防止システム (IPS) の削除

IPS 接続を削除できます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**トポロジー**」をクリックします。
3. デバイス・ノードとサブネット・ノードをつなぐ接続線にマウス・ポインターを移動します。
4. 接続線を右クリックし、「IPS idp の削除 (Remove IPS idp)」オプションを選択します。
5. 「**OK**」をクリックします。

トポロジー・デバイス・グループ

複雑なトポロジー・グラフを整理して単純化するには、 「トポロジー」ページでデバイスをグループ化します。

「現在のトポロジー (Current Topology)」ウィンドウでデバイスを選択してツールバーの「**アクション**」メニューをクリックするか、右クリック・メニューを使用して、デバイスの「**グループ**」機能にアクセスします。

トポロジー・グラフのレイアウト

トポロジー・レイアウトを現在のビューとして保存します。レイアウトを保存すると、トポロジーの現在のグラフィカル表現が保存されます。

「**アクション**」 > 「**レイアウト**」 > 「**レイアウトのリセット**」をクリックしてレイアウトをリセットするまで、保存したレイアウトがデフォルトのトポロジー画面になります。

レイアウトをリセットするときにこのレイアウトを保持する場合は、「**レイアウトの保存**」を選択します。

現在のトポロジーを PNG 画像または VDX 図面 (Visio XML) としてダウンロードするには、「**アクション**」 > 「**ダウンロード**」をクリックします。

第 6 章 ポリシー・モニター

組織はポリシー・モニターを使用して、ネットワークに関する具体的なリスクの質問を定義し、リスク・インディケーターの分析に基づいてリスクの評価または分析を行います。

ポリシー・モニターでは、ポリシーの定義、ポリシーの順守についての評価、質問の結果の評価、および新規リスクのモニターを行うことができます。

ネットワーク上のリスクを評価およびモニターするためのデフォルトの質問テンプレートが用意されています。独自の質問のベースとしてデフォルトの質問テンプレートのいずれかを使用することも、新しい質問を作成することもできます。デフォルトの質問テンプレートは、「ポリシー・モニター」ページの「**グループ**」メニューにあります。

選択できるリスク・インディケーターを以下にリストします。

- ネットワーク・アクティビティー。過去に発生したネットワーク通信に基づき、リスクを測定します。
- 構成およびトポロジー。可能な通信およびネットワーク接続に基づき、リスクを測定します。
- 脆弱性。ネットワーク・アセットから収集されたネットワーク構成データと脆弱点スキャン・データに基づき、リスクを測定します。
- ファイアウォール・ルール。ネットワーク全体に適用されるファイアウォール・ルールの有無に基づき、リスクを測定します。

リスク・インディケーターに基づくテストを定義した後、テスト結果を制限して、特定の結果または違反に対する照会をフィルタリングすることができます。

セキュリティーの専門家は、ネットワークのリスクにフラグを立てるために、アセットまたはデバイス/ルールに関する質問を作成します。質問をポリシー・モニターに送信すると、アセットまたはデバイス/ルールのリスク・レベルがレポートされます。アセットから返された結果を承認するか、承認されない結果に対するシステムの応答方法を定義できます。

質問の結果を使用して、多種多様なセキュリティーのシナリオでのリスクの事例を評価できます。例えば、以下について評価できます。

- ユーザーが禁止されているプロトコルを使用して通信を行ったかどうかを評価します。
- 特定のネットワーク上のユーザーが、禁止されているネットワークまたはアセットと通信できるかどうかを評価します。
- ファイアウォール・ルールが企業ポリシーと一致しているかどうかを評価します。
- ネットワーク構成の結果としてセキュリティーが侵害される可能性のあるシステムを評価し、脆弱性に優先順位を付けます。

© Copyright IBM Corp. 2012, 2015

ポリシー・モニターの質問

ポリシー・モニターで質問を定義することにより、ネットワーク・アクティビティー、脆弱性、ファイアウォール・ルールに基づいてリスクの評価とモニターを行うことができます。

質問を送信すると、以下のように選択したデータ・タイプに基づいてトポロジーが検索されます。

- アセットに基づく質問の場合、定義されたポリシーに違反するネットワーク・アセットまたはネットワークにリスクを生じさせたアセットに基づいて検索が実行されます。
- デバイスまたはルールに基づく質問の場合、定義されたポリシーに違反するデバイス内のルールまたはネットワークにリスクを生じさせたデバイス内のルールが検索によって特定されます。
- アセット・コンプライアンスに基づく質問の場合、アセットが CIS ベンチマークに準拠しているかどうかが検索によって特定されます。

注: 複数のドメインに対して IBM Security QRadar が構成されている場合、アセットの質問は、デフォルトのドメイン内のアセットだけをモニターします。アセット・コンプライアンスの質問は、「**管理**」 > 「**ドメイン管理**」ウィンドウで別のドメインが構成されていない限り、デフォルトのドメイン内のアセットをモニターします。ドメイン管理について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

デバイス/ルールの質問では、ルールおよびポリシーの違反が検索され、制限テスト・コンポーネントはありません。デバイス/ルールの質問でアプリケーションを検索することもできます。

アセットのテストは、以下のカテゴリーに分類されます。

- *寄与テスト* は、質問で指定されたリスク・インディケーターを検査するために質問パラメーターを使用します。生成されたリスク・データ結果は、*制限テスト* を使用してさらにフィルターに掛けることができます。寄与テストは、「**質問に含めるテストの指定 (Which tests do you want to include in your question)**」領域に表示されます。寄与テストは、テストの質問に一致する、検出されたアセットに基づいたデータを返します。
- *制限テスト* は、*寄与テスト* の質問で返される結果を絞り込みます。制限テストは、寄与テストの追加後に、「**質問に含めるテスト (Which tests do you want to include in your question)**」ウィンドウ内にのみ表示されます。寄与テストを質問に含めない限り、制限テストを追加することはできません。寄与テストの質問を削除した場合、制限テストの質問を保存することはできません。

アセット・コンプライアンスの質問は、CIS ベンチマークに準拠していないアセットを検索します。CIS ベンチマークに含めるテストは、コンプライアンス・ベンチマーク・エディターで構成します。

関連タスク:

48 ページの『質問の送信』
関連するリスクを判断するために、質問を送信します。質問の実行に必要な時間と、照会されるデータの量を判別することもできます。

49 ページの『コンプライアンス・ベンチマークの編集』
デフォルトの CIS ベンチマークにテストを追加したりテストを削除したりするには、IBM Security QRadar Risk Manager のコンプライアンス・ベンチマーク・エディターを使用します。

重要度係数

重要度係数は、リスク・スコアの計算、および質問に対して返される結果の数の定義に使用されます。

範囲は 1 (低重要度) から 10 (高重要度) までです。デフォルトは 5 です。

表 7. 重要度係数の結果マトリックス

重要度係数	アセット・テストで返される結果の数	デバイス/ルール・テストで返される結果の数
1 (低重要度)	10,000	1,000
10 (高重要度)	1	1

例えば、「**インターネットからの通信を受け入れたことがある、かつ、以下のネットワーク (DMZ) のみが含まれる (have accepted communication from the internet and include only the following networks (DMZ))**」というポリシーの質問では、高い重要度係数 10 が必要になります。この質問の内容はリスク性が高く、質問に対する結果が一切容認されないためです。一方、「インターネットからの通信を受け入れたことがある、かつ、以下のインバウンド・アプリケーション (P2P) のみが含まれる (have accepted communication from the internet and include only the following inbound applications (P2P))」というポリシーの質問の場合、質問の結果が高リスクを示さないため、重要度係数を低くしなければならない場合があります。ただし、情報提供を目的として、この通信をモニターする場合があります。

質問に関する情報の表示

ポリシー・モニターの質問とパラメーターに関する情報は、「ポリシー・モニター」ページで表示できます。

質問に関する詳細情報を表示する場合は、質問を選択すると、その説明を表示することができます。

選択時にその質問がモニター・モードになっている場合、選択した結果として生成されるイベントおよびオフェンスを確認できます。

アセットの質問の作成

定義済みのポリシーに違反しているネットワーク内のアセットや、リスクを生じさせているアセットを検索します。

このタスクについて

ポリシー・モニターの質問は、上から下へと評価されます。ポリシー・モニターの質問の順序は結果に影響を与えます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 「**アクション**」メニューから、「**新しいアセットの質問 (New Asset Question)**」を選択します。
4. 「**この質問の名前の指定 (What do you want to name this question)**」フィールドで、質問の名前を入力します。
5. 「**評価基準 (Evaluate On)**」リストから、以下のオプションのいずれかを選択します。

オプション	説明
実際の通信 (Actual Communication)	接続を使用する通信が検出されたすべてのアセットが含まれます。
通信の可能性 (Possible Communication)	ファイアウォールなどのネットワーク・トポロジーを通じて通信が許可されているすべてのアセットが含まれます。これらの質問を使用して、通信が検出されたかどうかにかかわらず、特定の通信が可能かどうかを調査します。

6. 「**重要度係数 (Importance Factor)**」リストから、この質問に関連付ける重要度のレベルを選択します。重要度係数は、リスク・スコアの計算、および質問に対して返される結果の数の定義に使用されます。
7. 質問の時刻範囲を指定します。
8. 「**質問に含めるテストの指定 (Which tests do you want to include in your question)**」フィールドで、含めるテストの横の追加 (+) アイコンを選択します。
9. テストのパラメーターを「**アセットの検出 (Find Assets that)**」フィールドで構成します。

   構成可能なパラメーターは太字かつ下線が付いています。各パラメーターをクリックして、質問について選択可能なオプションを表示します。
10. グループ域で、関係するチェック・ボックスをクリックし、グループ・メンバーシップをこの質問に割り当てます。
11. 「**質問の保存 (Save Question)**」をクリックします。

次のタスク

質問を送信してリスク要因を判別します。 48 ページの『質問の送信』を参照してください。

関連概念:

45 ページの『重要度係数』
重要度係数は、リスク・スコアの計算、および質問に対して返される結果の数の定義に使用されます。

61 ページの『質問のグループ化』
選択した基準に応じて質問をグループ化して表示できます。

デバイス内のルールをテストする質問の作成

「ポリシー・モニター」でデバイス/ルールの質問を作成して、定義済みのポリシーに違反したデバイス、またはネットワークにリスクを生じさせたデバイス内のルールを識別します。

このタスクについて

ポリシー・モニターの質問は、上から下へと評価されます。ポリシー・モニターの質問の順序は結果に影響を与えます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 「**アクション**」メニューから、「**新しいデバイス/ルールの質問 (New Device/Rules Question)**」をクリックします。
4. 「**この質問の名前の指定 (What do you want to name this question)**」フィールドで、質問の名前を入力します。
5. 「**重要度係数 (Importance Factor)**」リストから、この質問に関連付ける重要度のレベルを選択します。
6. 「**質問に含めるテストの指定 (Which tests do you want to include in your question)**」フィールドで、含めるテストの横の + アイコンをクリックします。
7. 「**次のデバイス/ルールを検出 (Find Devices/Rules that)**」フィールドで、テスト用のパラメーターを構成します。

   構成可能なパラメーターは太字かつ下線が付いています。各パラメーターをクリックして、質問について選択可能なオプションを表示します。
8. グループ域で、関係するチェック・ボックスをクリックし、グループ・メンバーシップをこの質問に割り当てます。
9. 「**質問の保存 (Save Question)**」をクリックします。

次のタスク

質問を送信してリスク要因を判別します。

関連概念:

45 ページの『重要度係数』
重要度係数は、リスク・スコアの計算、および質問に対して返される結果の数の定義に使用されます。

61 ページの『質問のグループ化』
選択した基準に応じて質問をグループ化して表示できます。

関連タスク:

48 ページの『質問の送信』
関連するリスクを判断するために、質問を送信します。質問の実行に必要な時間と、照会されるデータの量を判別することもできます。

質問の送信

関連するリスクを判断するために、質問を送信します。質問の実行に必要な時間と、照会されるデータの量を判別することもできます。

このタスクについて

質問を送信すると、結果として得られる情報は照会されるデータ (アセットまたはデバイスおよびルール) に応じたものになります。

ポリシー・モニターの質問を送信すると、質問の実行にかかる時間を確認できます。ポリシーの実行に必要な時間は、照会されるデータの量も示します。例えば、実行時間が 3 時間である場合には、3 時間分のデータがあることになります。モニターする質問に対して設定する効率的な間隔頻度を決定する際に、「**ポリシー実行時間 (Policy Execution Time)**」列で時間を確認できます。例えば、ポリシー実行時間が 3 時間である場合、ポリシー評価間隔は 3 時間より長くなければなりません。

注: 送信後に質問を編集し、その編集が関連するテストに影響を与える場合、その変更内容が表示されるには最大で 1 時間かかる可能性があります。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 送信する質問を選択します。
4. 「**質問の送信 (Submit Question)**」をクリックします。

アセット・コンプライアンスの質問の作成

CIS ベンチマーク・テストで不合格となるネットワーク内のアセットを検索するアセット・コンプライアンスの質問をポリシー・モニター内で作成します。

始める前に

ポリシー・モニターの質問は、上から下へと評価されます。ポリシー・モニターの質問の順序は結果に影響を与えます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 「**アクション**」メニューから、「**新しいアセット・コンプライアンスの質問 (New Asset Compliance Question)**」を選択します。
4. 「**この質問の名前の指定 (What do you want to name this question)**」フィールドで、質問の名前を入力します。
5. この質問に関連付ける重要度のレベルを「**重要度因子 (Importance Factor)**」リストから選択します。
6. 「**質問に含めるテストの指定 (Which tests do you want to include in your question)**」フィールドで、「**CIS ベンチマークの使用によるアセットの保存済み**

検索でアセットのコンプライアンスをテスト (test compliance of assets in asset saved searches with CIS benchmarks)」テストの横にある追加 (+) アイコンを選択します。

必要な場合、このテストを複数回選択します。

7. テストのパラメーターを「**アセットの検出 (Find Assets that)**」フィールドで構成します。

   各パラメーターをクリックして、質問について選択可能なオプションを表示します。必要な場合、複数のアセットの保存済み検索と複数のチェックリストをこのテストで指定します。

8. グループ域で、関係するチェック・ボックスをクリックし、グループ・メンバーシップをこの質問に割り当てます。

   アセット・コンプライアンスの質問は、コンプライアンス・ダッシュボードまたはレポートに含めるためにグループに割り当てておく必要があります。

9. 「**質問の保存 (Save Question)**」をクリックします。

次のタスク

作成した質問にベンチマーク・プロファイルを関連付け、質問の結果をモニターします。

関連概念:

45 ページの『重要度係数』
重要度係数は、リスク・スコアの計算、および質問に対して返される結果の数の定義に使用されます。

61 ページの『質問のグループ化』
選択した基準に応じて質問をグループ化して表示できます。

関連タスク:

50 ページの『アセット・コンプライアンスの質問のモニター』
アセット・コンプライアンスの質問は、CIS スキャン・プロファイルを選択してモニターします。 CIS ベンチマーク・スキャンは、アセットに対して実行します。

コンプライアンス・ベンチマークの編集

デフォルトの CIS ベンチマークにテストを追加したりテストを削除したりするには、IBM Security QRadar Risk Manager のコンプライアンス・ベンチマーク・エディターを使用します。

手順

1. 「**リスク**」タブをクリックします。
2. 「**ポリシー・モニター**」をクリックします。
3. 「**コンプライアンス**」をクリックして「コンプライアンス・ベンチマーク・エディター (Compliance Benchmark Editor)」ウィンドウを開きます。
4. ナビゲーション・メニューで、編集するデフォルトの CIS ベンチマークをクリックします。
5. 「**コンプライアンス**」ペインで、含める対象のテストに割り当てられている行の「**有効**」チェック・ボックスをクリックします。

テストを有効にする前に、行のいずれかの場所をクリックすると、ベンチマーク・テストの説明、デプロイメントの根拠、および検査対象についての情報が表示されます。

カスタム CIS チェックリストを作成する場合は、デフォルトでは含まれない一部のベンチマーク・テストの実行に長い時間がかかる可能性があることに注意してください。詳しくは、CIS の資料を参照してください。

次のタスク

編集したベンチマークに対してアセットをテストするアセット・コンプライアンスの質問を作成します。

関連タスク:

48 ページの『アセット・コンプライアンスの質問の作成』
CIS ベンチマーク・テストで不合格となるネットワーク内のアセットを検索するアセット・コンプライアンスの質問をポリシー・モニター内で作成します。

アセット・コンプライアンスの質問のモニター

アセット・コンプライアンスの質問は、CIS スキャン・プロファイルを選択してモニターします。 CIS ベンチマーク・スキャンは、アセットに対して実行します。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 「**質問**」ペインで、モニターするアセット・コンプライアンスの質問を選択します。
4. 「**モニター**」をクリックして、「結果のモニター」ウィンドウを開きます。
5. ベンチマーク・プロファイルを「**この質問に関連付けるベンチマーク・プロファイル (Which benchmark profile to associate with this question?)**」リストから選択します。

   選択されたベンチマーク・スキャン・プロファイルは、ドメインに関連付けられている QRadar Vulnerability Manager スキャナーを使用します。ドメイン・ネームは、「**ベンチマーク・プロファイルの詳細 (Benchmark Profile Details)**」領域に表示されます。ドメイン管理について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
6. 「**この質問/シミュレーションのモニター結果機能を有効にする (Enable the monitor results function for this question/simulation)**」チェック・ボックスを選択します。
7. 「**モニターの保存 (Save Monitor)**」をクリックします。

   モニターは、ベンチマーク・スキャン・プロファイルの作成時に「**スキャン時期 (When To Scan)**」タブで設定したスキャン開始時刻に開始されます。

関連タスク:

49 ページの『コンプライアンス・ベンチマークの編集』
デフォルトの CIS ベンチマークにテストを追加したりテストを削除したりするには、IBM Security QRadar Risk Manager のコンプライアンス・ベンチマーク・エデ

ィターを使用します。

48 ページの『アセット・コンプライアンスの質問の作成』
CIS ベンチマーク・テストで不合格となるネットワーク内のアセットを検索するアセット・コンプライアンスの質問をポリシー・モニター内で作成します。

ポリシー・モニターの質問のエクスポートおよびインポート

管理特権を持つユーザーは、ポリシー・モニターの質問をエクスポートおよびインポートできます。

質問のエクスポートおよびインポートは、質問をバックアップして、他の IBM Security QRadar Risk Manager ユーザーと共有する手段となります。

機密情報に関する制約事項

機密性の高い企業情報やポリシー情報が依存関係に含まれている場合があります。依存関係に含まれている機密データは、ポリシー・モニターの質問をエクスポートまたはインポートする際に除外されます。

ポリシー・モニターの質問には、以下のタイプの依存関係が含まれることがあります。

- アセット・ビルディング・ブロック
- アセットの保存済み検索
- ネットワーク
- リモート・ネットワーク・ロケーション
- 地理上のネットワーク・ロケーション
- リファレンス・セット

依存関係が含まれる質問をエクスポートするためには、依存関係に含まれる情報のタイプについて、追加のコンテキストを提供することもできます。この情報を示すことによって、他のユーザーがポリシー・モニターに質問をインポートする際に、情報のタイプを理解できるようになります。

ポリシー・モニターの質問のエクスポート

1 つ以上のポリシー・モニターの質問を XML ファイルにエクスポートできます。ポリシー・モニターの質問のエクスポートは、質問をバックアップしたり、他のユーザーと質問を共有したりする場合に便利です。

このタスクについて

ポリシー・モニターの質問に依存関係が含まれている場合は、依存関係に含まれている情報のタイプに関して詳細なコンテキストを提供できます。

エクスポートされた質問のデフォルトの XML ファイル名は、`policy_monitor_questions_export.xml` です。

手順

1. 「**リスク**」タブで、「**ポリシー・モニター**」をクリックします。
2. 次のオプションのいずれかを選択してください。
   - すべての質問をエクスポートするには、「**アクション**」メニューから、「**すべてをエクスポート (Export All)**」を選択します。
   - 選択した質問をエクスポートするには、Ctrl キーを押しながら、エクスポートする各質問を選択し、「**アクション**」メニューから「**選択済みをエクスポート (Export Selected)**」を選択します。
3. オプション。いずれかの質問に依存関係が含まれている場合は、パラメーター・リンクをクリックして、さらに具体的な情報を入力します。このフィールドの最大文字数は 255 文字です。
4. 「**質問をエクスポート (Export Questions)**」をクリックします。

タスクの結果

policy_monitor_questions_export.xml というデフォルトのファイルが、ダウンロード・ディレクトリーにエクスポートされます。

ポリシー・モニターの質問のインポート

1 つ以上のポリシー・モニターの質問を IBM Security QRadar Risk Manager にインポートできます。

このタスクについて

インポート・プロセスによって既存の質問が更新されることはありません。各質問はポリシー・モニターに新規の質問として表示されます。タイム・スタンプは、接尾部として、インポートされたすべての質問に追加されます。

インポートするポリシー・モニターの質問に依存関係が含まれている場合、この質問をインポートすると、警告が「**状況**」列に表示されます。インポートされた、依存関係がある質問には、値が指定されていないパラメーターが含まれています。インポートされたポリシー・モニターの質問を期待どおりに確実に機能させるには、値を空のパラメーターに割り当てる必要があります。

手順

1. 「**リスク**」タブで、「**ポリシー・モニター**」をクリックします。
2. 「**アクション**」メニューから、「**インポート**」を選択します。
3. 「**ファイルの選択 (Choose File)**」をクリックして、インポートする XML ファイルを参照して選択します。
4. 「**オープン**」をクリックします。
5. 1 つ以上のグループを選択して、質問をグループに割り当てます。
6. 「**質問のインポート (Import Question)**」をクリックします。
7. 「**状況**」列で警告を確認します。質問に警告が含まれている場合は、質問を開いて、依存関係があるパラメーターを編集します。パラメーターの編集を完了したら、質問を保存できます。

次のタスク

インポートされた質問に対するモニターは無効になっています。インポートされた質問の結果をモニターするには、イベントを作成できます。

アセットの結果

ポリシー・モニターの質問を送信した後に、アセットの結果が表示されます。

「リスク・スコア」により、質問に関連付けられたリスクのレベルが示されます。**「リスク・スコア」**は、質問に割り当てられた重要度係数と、質問に対して返された結果の数に基づいて計算されます。

アセットの結果のパラメーターについて、以下の表で説明します。

表 8. アセットの結果

パラメーター	説明
IP	アセットの IP アドレス。
名前	アセット・プロファイルから取得された、アセットの名前。 アセット・プロファイルについて詳しくは、「*IBM Security QRadar SIEM ユーザーズ・ガイド*」を参照してください。
VLAN	アセットに関連付けられた VLAN の名前。
重み	アセット・プロファイルから取得された、アセットの重み。
宛先ポート	質問のテストのコンテキストで、このアセットに関連付けられた宛先ポートのリスト。このアセットと質問に関連付けられたポートが複数ある場合、このフィールドには「複数」という語とポートの数が示されます。ポートのリストが取得される際には、この質問に関連付けられた接続がフィルタリングされ、アセットが送信元、宛先、または接続のいずれかであったときのすべての固有のポートが取得されます。 「複数 (N)」をクリックすると、接続が表示されます。この表示は、アセットの IP アドレスでフィルタリングされ、かつ、質問に指定された時間間隔に基づいた接続をポート別に集約して示します。

表 8. アセットの結果 (続き)

パラメーター	説明
プロトコル	質問のテストのコンテキストで、このアセットに関連付けられたプロトコルのリスト。このアセットと質問に関連付けられたプロトコルが複数ある場合、このフィールドには「複数」という語とプロトコルの数が示されます。プロトコルのリストが取得される際には、この質問に関連付けられた接続がフィルタリングされ、アセットが送信元、宛先、または接続のいずれかであったときのすべての固有のプロトコルが取得されます。 「複数 (N)」をクリックすると、接続が表示されます。この表示は、アセットの IP アドレスでフィルタリングされ、かつ、質問に指定された時間間隔に基づいた接続をプロトコル別に集約して示します。
フロー・アプリケーション	質問のテストのコンテキストで、このアセットに関連付けられたアプリケーションのリスト。このアセットと質問に関連付けられたアプリケーションが複数ある場合、このフィールドには「複数」という語とアプリケーションの数が示されます。アプリケーションのリストが取得される際には、この質問に関連付けられた接続がフィルタリングされ、アセットが送信元、宛先、または接続のいずれかであったときのすべての固有のアプリケーションが取得されます。 「複数 (N)」をクリックすると、接続が表示されます。この表示は、アセットの IP アドレスでフィルタリングされ、かつ、質問に指定された時間間隔に基づいた接続をアプリケーション別に集約して示します。

表 8. アセットの結果 (続き)

パラメーター	説明
脆弱性	質問のテストのコンテキストで、このアセットに関連付けられた脆弱性のリスト。このアセットと質問に関連付けられた脆弱性が複数ある場合、このフィールドには「複数」という語と脆弱性の数が示されます。 脆弱性のリストは、関連するテストからコンパイルされたすべての脆弱性のリストを使用し、このアセットで検出された脆弱性をフィルタリングすることで取得されます。質問に脆弱性が指定されていない場合は、このアセットのすべての脆弱性を使用して、脆弱性のリストがコンパイルされます。 「複数 (N)」をクリックすると、アセットが表示されます。この表示は、アセットの IP アドレスでフィルタリングされ、かつ、質問に指定された時間間隔に基づいた接続を脆弱性別に集約して示します。
フロー数	質問のテストのコンテキストで、このアセットに関連付けられたフローの合計数。 フロー数が決定される際には、この質問に関連付けられた接続がフィルタリングされ、アセットが送信元、宛先、または接続のいずれかであったときのフロー数の合計が取得されます。
送信元	質問のテストのコンテキストで、このアセットに関連付けられた送信元 IP アドレスのリスト。このアセットと質問に関連付けられた送信元 IP アドレスが複数ある場合、このフィールドには「複数」という用語と送信元 IP アドレスの数が示されます。送信元 IP アドレスのリストが取得される際には、この質問に関連付けられた接続がフィルタリングされ、アセットが接続の宛先であったときのすべての固有の送信元 IP アドレスが取得されます。 「複数 (N)」をクリックすると、接続が表示されます。この表示は、アセットの IP アドレスでフィルタリングされ、かつ質問に指定された時間間隔に基づいた接続を送信元 IP アドレス別に集約して示します。

表 8. アセットの結果 (続き)

パラメーター	説明
宛先	質問のテストのコンテキストで、このアセットに関連付けられた宛先 IP アドレスのリスト。このアセットと質問に関連付けられた宛先 IP アドレスが複数ある場合、このフィールドには「複数」という語と宛先 IP アドレスの数が示されます。宛先 IP アドレスのリストが取得される際には、質問に関連付けられた接続がフィルタリングされ、アセットが接続の送信元であるときのすべての固有の宛先 IP アドレスが取得されます。 「複数 (N)」をクリックすると、接続が表示されます。この表示は、アセットの IP アドレスでフィルタリングされ、かつ、質問に指定された時間間隔に基づいた接続を宛先 IP アドレス別に集約して示します。
フロー送信元バイト数	質問のテストのコンテキストで、このアセットに関連付けられた送信元バイト数の合計。 送信元バイト数が決定される際には、この質問に関連付けられた接続がフィルタリングされ、アセットが接続の送信元であったときの送信元バイト数の合計が取得されます。
フロー宛先バイト数	質問のテストのコンテキストで、このアセットに関連付けられた宛先バイト数の合計。 宛先バイト数が決定される際には、この質問に関連付けられた接続がフィルタリングされ、アセットが接続の宛先であったときの宛先バイト数の合計が取得されます。

デバイス/ルールの結果

ポリシー・モニターの質問を送信した後、デバイス/ルールの結果が表示されます。

表示される「**リスク・スコア**」は、質問に関連付けられたリスクのレベルを表します。「**リスク・スコア**」は、質問に割り当てられた重要度係数と、質問に対して返された結果の数に基づいて計算されます。

デバイスとルールの結果のパラメーターについて、以下の表で説明します。

表 9. デバイスおよびルールの結果

パラメーター	説明
デバイス IP	デバイスの IP アドレス。
デバイス名	構成モニターから取得された、デバイスの名前。

表 9. デバイスおよびルールの結果 (続き)

パラメーター	説明
デバイス・タイプ	アセット・プロファイルから取得された、デバイスのタイプ。 アセット・プロファイルについて詳しくは、「*IBM Security QRadar SIEM ユーザーズ・ガイド*」を参照してください。
リスト	デバイスのルールの名前。
項目	ルールの項目番号。
アクション	デバイスからの該当するルールに関連付けられたアクション。オプションは、許可、拒否、または該当なしです。
送信元	このアセットに関連付けられた送信元ネットワーク。 ハイパーリンク付きの送信元は、オブジェクト・グループ参照を示します。リンクをクリックすると、オブジェクト・グループ参照に関する詳細情報が表示されます。

送信元サービス	デバイスからの該当するルールに関連付けられた送信元ポートとそれに関する比較。次のフォーマットで示されます。
	
	`<comparison>:<port>`
	
	各部分の説明は次のとおりです。
	
	`<comparison>`
	
	以下のいずれかのオプションが含まれます。
	
	• eq - 等しい
	• ne - 等しくない
	• lt - より小さい
	• gt - より大きい
	
	例えば、パラメーターが ne:80 と示している場合、80 以外の任意のポートをこの送信元サービスに適用します。パラメーターが lt:80 と示している場合、適用可能なポートの範囲は、0 から 79 になります。
	
	このパラメーターは、デバイス・ルールの送信元ポートを表示します。デバイス・ルールに対するポートが存在しない場合は、「NA」という語が表示されます。
	
	ハイパーリンク付きの送信元サービスは、オブジェクト・グループ参照を示します。リンクをクリックすると、オブジェクト・グループ参照に関する詳細情報が表示されます。

表 9. デバイスおよびルールの結果 (続き)

パラメーター	説明
宛先	デバイスからの該当するルールに関連付けられた宛先ネットワーク。 ハイパーリンク付きの宛先は、オブジェクト・グループ参照を示します。リンクをクリックすると、オブジェクト・グループ参照に関する詳細情報が表示されます。

宛先サービス	デバイスからの該当するルールに関連付けられた宛先ポートとそれに関する比較が、次のフォーマットで示されます。
	
	`<comparison>:<port>`
	
	各部分の説明は次のとおりです。
	
	`<comparison>`
	
	以下のいずれかのオプションが含まれます。
	
	• eq - 等しい
	• ne - 等しくない
	• lt - より小さい
	• gt - より大きい
	
	例えば、パラメーターが ne:80 と示している場合、80 以外の任意のポートをこの宛先サービスに適用します。パラメーターが lt:80 と示している場合、適用可能なポートの範囲は、0 から 79 になります。
	
	このパラメーターは、デバイス・ルールの宛先ポートを表示します。デバイス・ルールに対するポートが存在しない場合は、「NA」という語が表示されます。
	
	ハイパーリンク付きの宛先サービスは、オブジェクト・グループ参照を示します。リンクをクリックすると、オブジェクト・グループ参照に関する詳細情報が表示されます。

ユーザー/グループ	デバイスからの該当するルールに関連付けられたユーザーまたはグループ。
プロトコル	デバイスからの該当するルールに関連付けられたプロトコルまたはプロトコルのグループ。
シグネチャー	デバイスのシグネチャー。IP デバイスのデバイス・ルールにのみ表示されます。
アプリケーション	デバイスからの該当するルールに関連付けられたアプリケーション。

ポリシー・モニターの質問の結果の評価

ポリシー・モニターの質問から返された結果を評価できます。

質問の結果を承認することは、質問の結果に関連付けられたアセットが安全であること、または今後は無視できることを IBMIBM Security QRadar Risk Manager に通知するようにシステムを調整することに相当します。

ユーザーがアセットの結果を承認すると、ポリシー・モニターはそのアセットの結果を承認済みと見なします。今後、ポリシー・モニターの質問が送信されるか、モニターされると、そのアセットは質問の結果にリストされなくなります。承認済みのアセットは、承認が取り消されない限り、質問の結果リストに表示されることはありません。ポリシー・モニターはネットワーク・セキュリティー管理者のために、ユーザー、デバイスの IP アドレス、承認の理由、適用可能なデバイス/ルール、日時を記録します。

結果の承認

返されたアセットまたはデバイス・ルールのリストを評価して、存在するリスクの程度を判断することができます。評価した後は、すべての結果または特定の結果を承認することができます。

手順

1. 結果の表で、受け入れる結果の横にあるチェック・ボックスを選択します。
2. 次のオプションのいずれかを選択してください。

オプション	説明
すべて承認 (Approve All)	このオプションを選択すると、すべての結果が承認されます。
選択した項目を承認 (Approve Selected)	承認する結果の横にあるチェック・ボックスを選択してから「選択した項目を承認 (Approve Selected)」をクリックします。

3. 承認の理由を入力します。
4. 「**OK**」をクリックします。
5. 「**OK**」をクリックします。
6. 質問に対する承認済みの結果を表示するには、「**承認済みの表示 (View Approved)**」をクリックします。

タスクの結果

「承認された質問の結果 (Approved Question Results)」ウィンドウに以下の情報が表示されます。

表 10. 「承認された質問の結果 (Approved question results)」のパラメーター

パラメーター	説明
デバイス/ルール	デバイス/ルールの質問に対する結果の場合は、この結果に関連したデバイスを示します。

表 10. 「承認された質問の結果 (Approved question results)」のパラメーター (続き)

パラメーター	説明
IP	アセットの質問に対する結果の場合は、アセットに関連した IP アドレスを示します。
承認者 (Approved By)	結果を承認したユーザー。
承認日時 (Approved On)	結果が承認された日時。
メモ	この結果に関連付けられたメモのテキストと、質問が承認された理由が表示されます。

結果の承認を取り消す場合は、承認を取り消すそれぞれの結果のチェック・ボックスを選択し、「**選択項目の取り消し (Revoke Selected)**」をクリックします。承認をすべて取り消すには、「**すべて取り消す (Revoke All)**」をクリックします。

質問のモニター

質問の結果が変更された場合にイベントが生成されるようにするには、モニター対象の質問を構成します。

モニター対象の質問を選択すると、IBM Security QRadar Risk Manager はその質問を継続的に分析し、質問の結果が変更されているかどうかを判別します。結果の変更を検出した場合、QRadar Risk Manager はオフェンスを生成して、ユーザーに定義済みポリシーからの逸脱を示すアラートを通知することができます。

モニター・モードの質問は、デフォルトで時刻範囲が 1 時間に設定されます。この値は、質問の作成時に設定された時間の値より優先されます。

結果をモニターするイベントの作成

ポリシー・モニターで作成した質問の結果をモニターするためのイベントを作成できます。

このタスクについて

イベントに対して構成するパラメーターを以下の表に示します。

表 11. 質問の結果のモニターのパラメーター

パラメーター	説明
ポリシー評価間隔 (Policy evaluation interval)	イベントを実行する間隔。
イベント名	「**ログ・アクティビティー**」タブおよび「**オフェンス**」タブに表示するイベントの名前。
イベントの説明	イベントの説明。この説明は、イベント詳細の「注釈」に表示されます。
上位カテゴリー	このルールでイベントを処理する際に使用する上位イベント・カテゴリー。
下位カテゴリー	このルールでイベントを処理する際に使用する下位イベント・カテゴリー。

表 11. 質問の結果のモニターのパラメーター (続き)

パラメーター	説明
ディスパッチされたイベントをオフェンスの一部にする	イベントを判定機能コンポーネントに転送します。オフェンスが生成されていない場合、新規オフェンスが作成されます。オフェンスが存在する場合、イベントが追加されます。 質問またはシミュレーションで相関付けた場合、質問のすべてのイベントが、単一のオフェンスに関連付けられます。 アセットで相関付けた場合、固有のアセットごとに、固有のオフェンスが作成または更新されます。
質問に合格したイベントをディスパッチする	ポリシー・モニターの質問に合格したイベントを判定機能コンポーネントに転送します。
脆弱性スコア調整 (Vulnerability Score Adjustments)	質問が不合格か合格かに応じて、アセットの脆弱性リスク・スコアを調整します。脆弱性リスク・スコアは、IBM Security QRadar Vulnerability Manager で調整されます。
追加のアクション (Additional Actions)	イベントを受信した際に実行する追加アクション。 複数の E メール・アドレスを入力する場合は、それぞれのアドレスをコンマで区切ってください。 このモニター対象の質問の結果として生成されたイベントをダッシュボードの「システム通知」項目に表示するには、「**通知**」を選択します。 syslog 出力の例を以下に示します。 `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`
モニターを有効にする (Enable Monitor)	質問をモニターします。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. モニターする質問を選択します。
4. 「**モニター**」をクリックします。
5. パラメーターの値を構成します。
6. 「**モニターの保存 (Save Monitor)**」をクリックします。

質問のグループ化

選択した基準に応じて質問をグループ化して表示できます。

質問を分類すると、効率的に質問を表示して追跡できるようになります。例えば、コンプライアンスに関連するすべての質問を表示することができます。

新規質問を作成する際に、その質問を既存のグループに割り当てることができます。

グループの表示

質問のグループを表示できます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 「**グループ**」リストから、表示するグループを選択します。

グループの作成

質問の新規グループを作成できます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 「**グループ (Groups)**」をクリックします。
4. メニュー・ツリーから、新しい下位グループを作成するグループを選択します。
5. 「**新規**」をクリックします。
6. 「**名前**」フィールドに、新規グループに割り当てる名前を指定します。名前の長さは 255 文字まで可能です。
7. 「**説明**」フィールドに、このグループに割り当てる説明を指定します。説明の長さは 255 文字まで可能です。
8. 「**OK**」をクリックします。
9. 新しいグループの場所を変更するには、新しいグループをクリックし、メニュー・ツリー内の任意の場所にフォルダーをドラッグします。

グループの編集

質問のグループを編集できます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 「**グループ (Groups)**」をクリックします。
4. メニュー・ツリーから、編集するグループを選択します。
5. 「**編集**」をクリックします。
6. 必要に応じて「**名前**」と「**説明**」を編集します。

   名前および説明のフィールドの最大長は 255 文字です。
7. 「**OK**」をクリックします。
8. グループの場所を変更するには、グループをクリックし、メニュー・ツリー内の任意の場所にフォルダーをドラッグします。
9. 「グループ」ウィンドウを閉じます。

別のグループへの項目のコピー

グループ機能を使用して、シミュレーションを 1 つまたは多数のグループにコピーすることができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 「**グループ (Groups)**」をクリックします。
4. メニュー・ツリーから、別のグループにコピーする質問を選択します。
5. 「**コピー**」をクリックします。
6. シミュレーションのコピー先のグループのチェック・ボックスを選択します。
7. 「**コピー**」をクリックします。

グループからの項目の削除

項目をグループから削除することができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 「**グループ (Groups)**」をクリックします。
4. メニュー・ツリーから最上位グループを選択します。
5. グループのリストから、削除する項目またはグループを選択します。
6. 「**削除**」をクリックします。
7. 「**OK**」をクリックします。

項目のグループへの割り当て

質問をグループに割り当てることができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. グループに割り当てる質問を選択します。
4. 「**アクション**」メニューを使用して「**グループの割り当て**」を選択します。
5. 質問を割り当てるグループを選択します。
6. 「**グループの割り当て**」をクリックします。

IBM Security QRadar Risk Manager と IBM Security QRadar Vulnerability Manager の統合

IBM Security QRadar Vulnerability Manager を QRadar Risk Manager と統合すると、ネットワークのリスクおよび脆弱性に優先順位を付けることができます。

リスク・ポリシーおよび脆弱性の優先順位付け

QRadar Vulnerability Manager を QRadar Risk Manager と統合するには、アセットまたは脆弱性リスク・ポリシーを定義してモニターします。

QRadar Risk Manager で定義するリスク・ポリシーに合格するか不合格になると、QRadar Vulnerability Manager の脆弱性リスク・スコアが調整されます。調整レベルは、組織のリスク・ポリシーによって決まります。

QRadar Vulnerability Manager で脆弱性リスク・スコアが調整されるとき、管理者は以下の作業を実行できます。

- リスク・ポリシーに不合格になった脆弱性を直ちに可視化する。

  例えば、新しい情報を QRadar ダッシュボードに表示したり、E メールを使用して送信したりすることができます。
- 直ちに対処する必要がある脆弱性の優先順位を付け直す。

  例えば、管理者は「**リスク・スコア**」を使用してハイリスクの脆弱性を迅速に見分けることができます。

QRadar Risk Manager でアセット・レベルでリスク・ポリシーを適用すると、そのアセットのすべての脆弱性のリスク・スコアが調整されます。

ポリシー・モニターのユース・ケース

リスクについてネットワークを分析するための質問を作成する際には、多数のオプションを使用できます。

以下のポリシー・モニターの例で、ネットワーク環境で使用できる共通ユース・ケースの概要を説明します。

保護アセットで可能な通信を対象としたアセット・テスト

このユース・ケースでは、IP アドレスに基づいてポリシー・モニターの質問を作成する方法を示します。どのような組織にも、トラフィックをモニターし、信頼できる従業員のみがアクセスできるようにしている、重要なサーバーが含まれるネットワークが存在します。

このタスクについて

リスクの観点からは、組織内のユーザーのうち、重要なネットワーク・アセットと通信できるユーザーを把握しておくことが重要です。IBM Security QRadar Risk Manager は、そのために、可能な通信のアセット・テストに基づいてポリシー・モニターの質問を作成します。

このようなユース・ケースでの目的のためにポリシー・モニターの質問を作成する方法がいくつかあります。重要なサーバーへのすべての接続を時系列で表示できますが、地域の従業員がこれらの重要なサーバーにアクセスしていないことに注意を払いたい場合もあります。そのために、IP アドレスによってネットワークのトポロジーを参照するポリシー・モニターの質問を作成できます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 「**アクション**」メニューから、「**新規**」を選択します。
4. 「**この質問の名前の指定 (What do you want to name this question)**」フィールドで、質問の名前を入力します。
5. 「**返すデータのタイプの指定 (What type of data do you want to return)**」ドロップダウン・リストで「アセット」を選択します。
6. 「**評価基準 (Evaluate On)**」ドロップダウン・リストから「可能な通信 (Possible Communication)」を選択します。
7. 「**重要度係数 (Importance Factor)**」ドロップダウン・リストで、質問に関連付ける重要度のレベルを指定します。
8. 「**時刻範囲**」セクションで、質問の時刻範囲を指定します。
9. 「**質問に含めるテスト (Which tests do you want to include in your question)**」セクションで「**宛先アセット・ビルディング・ブロックへの通信が受け入れられたことがある (have accepted communication to destination asset building blocks)**」をダブルクリックして選択します。
10. 「次のアセットを検出 (Find Assets that)」セクションで「**アセット・ビルディング・ブロック**」をクリックし、このテストを詳細に構成し、「**保護アセット (Protected Assets)**」を指定します。

    注: ネットワーク・リモート・アセットを定義するには、事前にリモート・アセットのビルディング・ブロックを定義しておく必要があります。
11. 「**質問に含めるテスト (Which tests do you want to include in your question)**」セクションで、制限テスト「**以下の IP アドレスのみを含める (include only the following IP addresses)**」をダブルクリックして選択します。
12. 「次のアセットを検出 (Find Assets that)」セクションで、「**IP アドレス**」をクリックします。
13. リモート・ネットワークの IP アドレス範囲または CIDR アドレスを指定します。
14. 「**質問の保存 (Save Question)**」をクリックします。
15. 保護アセットに対して作成したポリシー・モニターの質問を選択します。
16. 「**質問の送信 (Submit Question)**」をクリックします。
17. 結果を確認して、不明な IP アドレスまたは CIDR 範囲からの通信を保護アセットが受け入れたかどうかを調べます。
18. オプション。結果を適切に調整した後、その質問をモニター・モードに変更して、保護されたアセットをモニターできます。認識されない IP アドレスから保護アセットが接続されている場合、QRadar Risk Manager でアラートを生成できます。

次のタスク

質問をモニターできます。

インターネット・アクセスのデバイス/ルール・テスト通信

このユース・ケースでは、デバイス/ルールに基づいてポリシー・モニターの質問を作成する方法を示します。デバイス・テストは、定義済みポリシーに違反するデバイス内のルールや、環境にリスクを生じさせた変更を識別します。

このタスクについて

デバイス・テストは、定義済みポリシーに違反するデバイス内のルールや、環境にリスクを生じさせた変更を識別します。ネットワークの観点から、どのデバイス・ルールが変更された可能性があるかを識別し、修正できるようにそのルールについてのアラートを受け取れるようにしておくことが重要です。非常によく発生する例としては、以前はインターネットにアクセスできなかったサーバーが、ネットワーク上のファイアウォールの変更が原因でアクセス権限を付与されてしまう場合があります。IBM Security QRadar Risk Manager では、デバイス・ルールに基づいてポリシー・モニターの質問を作成することにより、ネットワーク・デバイスのルール変更をモニターすることができます。

このようなユース・ケースでの目的のためにポリシー・モニターの質問を作成する方法がいくつかあります。以下の例では、どのデバイスがインターネットにアクセス可能かを確認するポリシー・モニターの質問を作成します。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 「**アクション**」メニューから、「**新規**」を選択します。
4. 「**返すデータのタイプの指定 (What type of data do you want to return)**」ドロップダウン・リストで、「デバイス/ルール (Devices/Rules)」を選択します。
5. 「**重要度係数 (Importance Factor)**」ドロップダウン・リストで、質問に関連付ける重要度のレベルを指定します。
6. 「**質問に含めるテストの指定 (Which tests do you want to include in your question)**」セクションで、「**インターネットへの接続を許可 (allow connection to the internet)**」をダブルクリックして選択します。
7. 「**質問の保存 (Save Question)**」をクリックします。
8. デバイス・ルールのモニター用に作成したポリシー・モニターの質問を選択します。
9. 「**質問の送信 (Submit Question)**」をクリックします。
10. 結果をレビューして、インターネットへのアクセスを許可しているルールがあるかどうかを確認します。
11. オプション。結果を適切に調整した後、その質問をモニター・モードに変更して、保護されたアセットをモニターできます。

次のタスク

質問をモニターできます。

リスク・ポリシーの適用による高リスク脆弱性の優先順位付け

IBM Security QRadar Vulnerability Manager では、脆弱性にリスク・ポリシーを適用することにより、高リスク脆弱性についてのアラートを管理者に通知できます。

リスク・ポリシーを適用すると、脆弱性のリスク・スコアが調整されるため、管理者は、即時に対応する必要がある脆弱性の優先順位をより正確に設定できます。

この例では、40 日後もネットワーク上でアクティブなままの脆弱性に対して、脆弱性リスク・スコアが所定のパーセンテージ係数分だけ自動的に増加します。

手順

1. 「**脆弱性**」タブをクリックします。
2. ナビゲーション・ペインで、「**脆弱性の管理**」をクリックします。
3. ツールバーで、「**検索**」 > 「**新規検索**」をクリックします。
4. 「検索パラメーター」ペインで、以下のフィルターを構成します。
   a. **リスクが高と等しい (Risk Equals High)**
   b. **脆弱性の検出以降の日数が 40 以上である (Days since vulnerabilities discovered Greater than or equal to 40)**
5. 「**検索**」をクリックし、ツールバーで、「**検索条件の保存**」をクリックします。

   QRadar Risk Manager 内で識別可能な保存済み検索名を入力します。
6. 「**リスク**」タブをクリックします。
7. ナビゲーション・ペインで、「**ポリシー・モニター**」をクリックします。
8. ツールバーで、「**アクション**」 > 「**新規**」をクリックします。
9. 「**この質問の名前の指定 (What do you want to name this question)**」フィールドで、名前を入力します。
10. 「**質問に含めるテストの指定 (Which tests do you want to include in your question)**」フィールドで、「**脆弱性の保存済み検索内に含まれる脆弱性の影響を受けやすい (are susceptible to vulnerabilities contained in vulnerability saved searches)**」をクリックします。
11. 「**アセットの検出 (Find Assets that)**」フィールドで、「**脆弱性の保存済み検索内に含まれる脆弱性の影響を受けやすい (are susceptible to vulnerabilities contained in vulnerability saved searches)**」で下線の付いたパラメーターをクリックします。
12. QRadar Vulnerability Manager 高リスク脆弱性の保存済み検索を識別し、「**追加**」をクリックし、「**OK**」をクリックします。
13. 「**質問の保存 (Save Question)**」をクリックします。
14. 「質問」ペインで、リストから質問を選択し、ツールバーで、「**モニター**」をクリックします。

    制約事項: 「**イベントの説明**」フィールドは必須です。
15. 「**質問に合格したイベントをディスパッチする**」をクリックします。

16. 「**脆弱性スコアの調整**」フィールドに、「**質問失敗時のパーセンテージ脆弱性スコアの調整 (Percentage vulnerability score adjustment on question fail)**」フィールド内のリスク調整パーセンテージ値を入力します。
17. 「**アセット上のすべての脆弱性に調整を適用 (Apply adjustment to all vulnerabilities on an asset)**」をクリックし、「**モニターの保存 (Save Monitor)**」をクリックします。

次のタスク

「**脆弱性**」タブで、高リスク脆弱性を検索し、脆弱性の優先順位を設定することができます。

DMZ 許可プロトコルの実際の通信

このユース・ケースでは、DMZ の信頼できるプロトコルの既知のリストに基づいてポリシー・モニターの質問を作成する方法を示します。ほとんどの組織では、DMZ を通過するネットワーク・トラフィックを、指定されたポートでの既知の信頼できるプロトコル (HTTP や HTTPS など) に制限します。

このタスクについて

リスクの観点から、DMZ でのトラフィックを継続的にモニターして、信頼できるプロトコルのみが存在することを確認することが重要です。IBM Security QRadar Risk Manager は、そのために、実際の通信のアセット・テストに基づいてポリシー・モニターの質問を作成します。

このようなユース・ケースでの目的のためにポリシー・モニターの質問を作成する方法がいくつかあります。ネットワーク・ポリシーでは少数の信頼できるプロトコルしか許可されないことが明らかなため、DMZ の信頼できるプロトコルの既知のリストに基づいてポリシー・モニターの質問を作成するオプションを選択します。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 「**アクション**」メニューから、「**新規**」を選択します。
4. 「**この質問の名前の指定 (What do you want to name this question)**」フィールドで、質問の名前を入力します。
5. 「**返すデータのタイプの指定 (What type of data do you want to return)**」ドロップダウン・リストで「アセット」を選択します。
6. 「**評価基準 (Evaluate On)**」ドロップダウン・リストから「実際の通信 (Actual Communication)」を選択します。
7. 「**重要度係数 (Importance Factor)**」ドロップダウン・リストで、質問に関連付ける重要度のレベルを指定します。
8. 「**時刻範囲**」セクションで、質問の時刻範囲を指定します。
9. 「**質問に含めるテスト (Which tests do you want to include in your question)**」セクションで「**宛先ネットワークへの通信が受け入れられたことがある (have accepted communication to destination networks)**」を選択します。

10. 「**次のアセットを検出 (Find Assets that)**」セクションで「**宛先ネットワーク**」をクリックし、このテストを詳細に構成して、宛先ネットワークとして DMZ を指定します。
11. 「**以下のインバウンド・ポートを含める (and include the following inbound ports)**」を選択します。
12. 「**次のアセットを検出 (Find Assets that)**」セクションで、「次のみを含める (include only)」パラメーターをクリックします (「次を除外 (exclude)」に変化します)。パラメーターが表示され、「次を除外: 以下のインバウンド・ポート (exclude the following inbound ports)」になります。
13. 「**ポート**」をクリックします。
14. ポート 80 および 443 を追加して「**OK**」をクリックします。
15. 「**質問の保存 (Save Question)**」をクリックします。
16. 作成したポリシー・モニター DMZ の質問を選択します。
17. 「**質問の送信 (Submit Question)**」をクリックします。
18. 結果を確認して、ポート 80 およびポート 443 以外のプロトコルによる通信がネットワークで行われているかどうかを調べます。
19. オプション。結果を適切に調整したら、質問をモニター・モードに変更することで DMZ の質問をモニターすることができます。

次のタスク

質問をモニターできます。

CIS ベンチマーク・スキャン

CIS ベンチマーク・スキャンをセットアップするには、QRadar の「管理」、「アセット」、「脆弱性」、および「リスク」の各タブで、一連の構成タスクを実行する必要があります。

CIS ベンチマーク・スキャンをセットアップするには、以下の前提条件が必要です。

IBM Security QRadar Vulnerability Manager および IBM Security QRadar Risk Manager の有効なライセンス

旧バージョンの IBM Security QRadar からのパッチを適用した場合は、CIS ベンチマーク・スキャンを実行する前に自動更新を行う必要があります。

CIS ベンチマーク・スキャンのセットアップに関連するステップは、以下の 8 つです。

1. アセットの追加。
2. 資格情報セットの構成。

   最も簡単な方法は、IBM Security QRadar の「管理」タブで、集中管理された資格情報を追加することですが、ベンチマーク・プロファイルの作成時に資格情報を追加することもできます。
3. アセットの保存済み検索の作成。

アセットの保存済み検索は、アセット・コンプライアンスの質問を構成する際に使用します。

4. QRadar Vulnerability Manager での CIS ベンチマーク・チェックの変更。

   コンプライアンス・ベンチマーク・エディターを使用して、カスタム CIS ベンチマーク・チェックリストを作成できます。

5. QRadar Vulnerability Manager での CIS ベンチマーク・スキャン・プロファイルの構成。
6. IBM Security QRadar Risk Manager でのアセット・コンプライアンスの質問の作成。
7. 作成したアセット・コンプライアンスの質問のモニター。
8. CIS ベンチマーク・スキャン結果の表示。

アセット・プロファイルの追加または編集

CIS ベンチマーク・スキャンを実行するには、スキャンするネットワーク・アセットを IBM Security QRadar に追加する必要があります。アセット・プロファイルは自動的にディスカバーおよび追加されます。ただし、プロファイルを手動で追加する必要がある場合があります。

このタスクについて

各アセットの情報を手動で入力するには、「**アセット**」タブでアセット・プロファイルを作成します。また、「**脆弱性**」タブでスキャン・プロファイルを構成することでディスカバリー・スキャンを実行することもできます。ディスカバリー・スキャンにより、QRadar® が、重要なアセット特性 (オペレーティング・システム、デバイス・タイプ、サービスなど) を識別することができます。

「サーバー・ディスカバリー」オプションを使用してアセットがディスカバーされると、一部のアセット・プロファイルの詳細が自動的に取り込まれます。アセット・プロファイルには情報を手動で追加して、特定のパラメーターを編集することができます。

編集できるのは、手動で入力されたパラメーターのみです。システムによって生成されたパラメーターはイタリックで表示され、編集できません。システム生成パラメーターは必要に応じて削除することができます。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 次のオプションのいずれかを選択してください。
   - アセットを追加するには、「**アセットの追加**」をクリックして、「**新規 IP アドレス**」フィールドにアセットの IP アドレスまたは CIDR 範囲を入力します。
   - アセットを編集するには、表示するアセットをダブルクリックして、「**アセットの編集**」をクリックします。
4. 「MAC および IP アドレス (MAC & IP Address)」ペインでパラメーターを構成します。次の 1 つ以上のオプションを構成してください。

- 「**新規 MAC アドレス**」アイコンをクリックして、ダイアログ・ボックスに MAC アドレスを入力します。
- 「**新規 IP アドレス**」アイコンをクリックして、ダイアログ・ボックスに IP アドレスを入力します。
- 「**不明な NIC**」がリストされている場合は、この項目を選択し、「**編集**」アイコンをクリックして、ダイアログ・ボックスに新しい MAC アドレスを入力できます。
- リストから MAC アドレスまたは IP アドレスを選択し、「**編集**」アイコンをクリックして、ダイアログ・ボックスに新しい MAC アドレスを入力します。
- リストから MAC アドレスまたは IP アドレスを選択して、「**削除**」アイコンをクリックします。

5. 「名前および説明 (Names & Description)」ペインでパラメーターを構成します。次の 1 つ以上のオプションを構成してください。

パラメーター	**説明**
DNS	次のオプションのいずれかを選択してください。 • DNS 名を入力して、「**追加**」をクリックします。 • リストから DNS 名を選択して、「**編集**」をクリックします。 • リストから DNS 名を選択して、「**削除**」をクリックします。
NetBIOS	次のオプションのいずれかを選択してください。 • NetBIOS 名を入力して、「**追加**」をクリックします。 • リストから NetBIOS 名を選択して、「**編集**」をクリックします。 • リストから NetBIOS 名を選択して、「**削除**」をクリックします。
指定された名前 (Given Name)	このアセット・プロファイルの名前を入力します。
ロケーション (Location)	このアセット・プロファイルのロケーションを入力します。
説明	アセット・プロファイルの説明を入力します。
ワイヤレス AP (Wireless AP)	このアセット・プロファイルのワイヤレス・アクセス・ポイント (AP) を入力します。
ワイヤレス SSID (Wireless SSID)	このアセット・プロファイルのワイヤレス・サービス・セット ID (SSID) を入力します。
スイッチ ID (Switch ID)	このアセット・プロファイルのスイッチ ID を入力します。
スイッチ・ポート ID (Switch Port ID)	このアセット・プロファイルのスイッチ・ポート ID を入力します。

6. 「オペレーティング・システム (Operating System)」ペインで、以下のようにパラメーターを構成します。
   a. 「**ベンダー**」リスト・ボックスから、オペレーティング・システム・ベンダーを選択します。
   b. 「**製品**」リスト・ボックスから、アセット・プロファイルのオペレーティング・システムを選択します。
   c. 「**バージョン**」リスト・ボックスから、選択したオペレーティング・システムのバージョンを選択します。
   d. 「**追加**」アイコンをクリックします。
   e. 「**オーバーライド**」リスト・ボックスから、以下のいずれかのオプションを選択します。
      - **次のスキャンまで (Until Next Scan)** - このオプションを選択すると、スキャナーによってオペレーティング・システム情報が提供され、情報を一時的に編集できるように指定されます。オペレーティング・システムのパラメーターを編集すると、スキャナーによって、その次のスキャンで情報がリストアされます。
      - **無制限 (Forever)** - 手動でオペレーティング・システム情報を入力する必要があり、スキャナーによって情報が更新されないように指定するには、このオプションを選択します。
   f. リストからオペレーティング・システムを選択します。
   g. オペレーティング・システムを選択して、「**オーバーライドの切り替え (Toggle Override)**」アイコンをクリックします。
7. 「CVSS および重み (CVSS & Weight)」ペインでパラメーターを構成します。次の 1 つ以上のオプションを構成してください。

パラメーター	説明
二次的被害の可能性	このアセットの損害または窃盗によるライフまたは物理アセットの損失の可能性を示すように、このパラメーターを構成します。このパラメーターを使用して、生産性または収益の経済的損失の可能性を示すこともできます。二次的被害の可能性が増えると、「CVSS スコア」パラメーターの計算値が増えます。 「**二次的被害の可能性**」リスト・ボックスから、以下のいずれかのオプションを選択します。 • なし • 低 • 低から中 • 中から高 • 高 • 未定義 「**二次的被害の可能性**」パラメーターを構成すると、「**重み**」パラメーターが自動的に更新されます。
機密性要件	このアセットの脆弱性をエクスプロイトされた場合の機密性への影響を示すように、このパラメーターを構成します。機密性への影響が増すと、「CVSS スコア」パラメーターの計算値が増えます。 「**機密性要件**」リスト・ボックスから、以下のいずれかのオプションを選択します。 • 低 • 中 • 高 • 未定義

パラメーター	説明
可用性要件	脆弱性をエクスプロイトされた場合のアセットの可用性への影響を示すように、このパラメーターを構成します。ネットワーク帯域幅、プロセッサー・サイクル、またはディスク・スペースを消費する攻撃は、アセットの可用性に影響します。可用性への影響が増すと、「CVSS スコア」パラメーターの計算値が増えます。 「**可用性要件**」リスト・ボックスから、以下のいずれかのオプションを選択します。 • 低 • 中 • 高 • 未定義
整合性要件	脆弱性をエクスプロイトされた場合のアセットの保全性への影響を示すには、このパラメーターを構成します。保全性とは、情報の信頼性および保証された信憑性を意味します。保全性への影響が増すと、「CVSS スコア」パラメーターの計算値が増えます。 「**整合性要件**」リスト・ボックスから、以下のいずれかのオプションを選択します。 • 低 • 中 • 高 • 未定義
重み	「**重み**」リスト・ボックスから、このアセット・プロファイルの重みを選択します。範囲は 0 から 10 です。 「**重み**」パラメーターを構成すると、「**二次的被害の可能性**」パラメーターが自動的に更新されます。

8. 「所有者 (Owner)」ペインでパラメーターを構成します。次の 1 つ以上のオプションを選択してください。

パラメーター	説明
ビジネス・オーナー (Business Owner)	アセットのビジネス・オーナーの名前を入力します。ビジネス・オーナーの例として、部長などがあります。最大長は 255 文字です。
ビジネス・オーナーの連絡先 (Business Owner Contact)	ビジネス・オーナーの連絡先情報を入力します。最大長は 255 文字です。

パラメーター	説明
テクニカル・オーナー	アセットのテクニカル・オーナーを入力します。テクニカル・オーナーの例として、IT マネージャーやディレクターなどがあります。最大長は 255 文字です。
テクニカル・オーナーの連絡先	テクニカル・オーナーの連絡先情報を入力します。最大長は 255 文字です。
テクニカル・ユーザー (Technical User)	リスト・ボックスから、このアセット・プロファイルに関連付けるユーザー名を選択します。 このパラメーターを使用して、IBM Security QRadar Vulnerability Manager の脆弱性の自動修復を有効にすることができます。自動修復について詳しくは、「*IBM Security QRadar Vulnerability Manager User Guide*」を参照してください。

9. 「**保存**」をクリックします。

資格情報セットの構成

IBM Security QRadar Vulnerability Manager で、ネットワーク内のアセットに対して資格情報セットを作成できます。スキャンの実行中に、スキャン・ツールで Linux、UNIX、または Windows オペレーティング・システムの資格情報が必要となった場合は、資格情報セットからスキャン・ツールへ自動的に資格情報が渡されます。

手順

1. 「**管理**」タブをクリックします。
2. 「**システム構成**」ペインで、「**集中管理された資格情報**」をクリックします。
3. 「集中管理された資格情報」ウィンドウのツールバーで、「**追加**」をクリックします。

   資格情報セットを構成する場合、「資格情報セット」ウィンドウの必須フィールドは「**名前**」フィールドのみです。
4. 「資格情報セット」ウィンドウで、「**アセット**」タブをクリックします。
5. 資格情報を指定するアセットの CIDR 範囲を入力し、「**追加**」をクリックします。
6. オプション: 「**Linux/Unix**」、「**Windows**」、「**ネットワーク・デバイス (SNMP)**」のいずれかのタブをクリックし、資格情報を入力します。
7. 「**保存**」をクリックします。

アセット検索条件の保存

「**アセット**」タブでは、構成済み検索条件を再使用できるように保存することができます。保存済み検索条件の有効期限が切れることはありません。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 検索を実行します。
4. 「**条件の保存**」をクリックします。
5. 次の各パラメーターの値を入力します。

パラメーター	説明
この検索の名前を入力してください (Enter the name of this search)	この検索条件に割り当てる固有名を入力します。
グループの管理	検索グループを管理するには、「**グループの管理**」をクリックします。このオプションは、管理権限がある場合にのみ表示されます。
グループへの検索の割り当て	この保存済み検索を割り当てるグループのチェック・ボックスを選択します。グループを選択しない場合、この保存済み検索はデフォルトで「**その他**」グループに割り当てられます。
クイック検索に含める	この検索を「**クイック検索**」リスト・ボックス (「**アセット**」タブ・ツールバーにあります) に含める場合は、このチェック・ボックスを選択します。
デフォルトとして設定	「**アセット**」タブへのアクセス時にこの検索をデフォルトとして設定する場合は、このチェック・ボックスを選択します。
全員と共有	検索要件をすべてのユーザーと共有する場合は、このチェック・ボックスを選択します。

コンプライアンス・ベンチマークの編集

デフォルトの CIS ベンチマークにテストを追加したりテストを削除したりするには、IBM Security QRadar Risk Manager のコンプライアンス・ベンチマーク・エディターを使用します。

手順

1. 「**リスク**」タブをクリックします。
2. 「**ポリシー・モニター**」をクリックします。
3. 「**コンプライアンス**」をクリックして「コンプライアンス・ベンチマーク・エディター (Compliance Benchmark Editor)」ウィンドウを開きます。
4. ナビゲーション・メニューで、編集するデフォルトの CIS ベンチマークをクリックします。
5. 「**コンプライアンス**」ペインで、含める対象のテストに割り当てられている行の「**有効**」チェック・ボックスをクリックします。

テストを有効にする前に、行のいずれかの場所をクリックすると、ベンチマーク・テストの説明、デプロイメントの根拠、および検査対象についての情報が表示されます。

カスタム CIS チェックリストを作成する場合は、デフォルトでは含まれない一部のベンチマーク・テストの実行に長い時間がかかる可能性があることに注意してください。詳しくは、CIS の資料を参照してください。

次のタスク

編集したベンチマークに対してアセットをテストするアセット・コンプライアンスの質問を作成します。

関連タスク:

48 ページの『アセット・コンプライアンスの質問の作成』

CIS ベンチマーク・テストで不合格となるネットワーク内のアセットを検索するアセット・コンプライアンスの質問をポリシー・モニター内で作成します。

ベンチマーク・プロファイルの作成

Center for Internet Security コンプライアンス・スキャンを作成するには、ベンチマーク・プロファイルを構成する必要があります。CIS コンプライアンス・スキャンを使用して、Windows および Red Hat Enterprise Linux CIS ベンチマーク・コンプライアンスをテストします。

手順

1. 「**脆弱性**」タブをクリックします。
2. ナビゲーション・ペインで、「**管理**」 > 「**スキャン・プロファイル**」をクリックします。
3. ツールバーで、「**ベンチマークの追加 (Add Benchmark)**」をクリックします。
4. 定義済みの集中管理された資格情報を使用する場合、「**集中管理された資格情報を使用 (Use Centralized Credentials)**」チェック・ボックスを選択します。

   Linux オペレーティング・システムのスキャンに使用される資格情報は、root 特権を持つ必要があります。Windows オペレーティング・システムのスキャンに使用される資格情報は、管理者特権を持つ必要があります。
5. 動的スキャンを使用していない場合は、「**スキャン・サーバー (Scan Server)**」リストから QRadar Vulnerability Manager スキャナーを選択します。
6. 動的スキャンを有効にするには、「**動的サーバーの選択 (Dynamic server selection)**」チェック・ボックスをクリックします。

   「**管理**」 > 「**ドメイン管理**」ウィンドウでドメインを構成した場合は、「**ドメイン**」リストからドメインを選択できます。CIDR 範囲内のアセットおよびスキャナーに対して構成されたドメインのみがスキャンされます。
7. 「**スキャン時期 (When To Scan)**」タブで、実行スケジュール、スキャン開始時刻、および事前定義される操作可能ウィンドウを設定します。
8. 「**E メール**」タブで、このスキャンについて送信する情報の内容と送信先を定義します。

9. 集中管理された資格情報を使用しない場合、スキャンで必要となる資格情報を「**追加の資格情報 (Additional Credentials)**」タブで追加します。

   Linux オペレーティング・システムのスキャンに使用される資格情報は、root 特権を持つ必要があります。Windows オペレーティング・システムのスキャンに使用される資格情報は、管理者特権を持つ必要があります。

10. 「**保存**」をクリックします。

アセット・コンプライアンスの質問の作成

CIS ベンチマーク・テストで不合格となるネットワーク内のアセットを検索するアセット・コンプライアンスの質問をポリシー・モニター内で作成します。

始める前に

ポリシー・モニターの質問は、上から下へと評価されます。ポリシー・モニターの質問の順序は結果に影響を与えます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 「**アクション**」メニューから、「**新しいアセット・コンプライアンスの質問 (New Asset Compliance Question)**」を選択します。
4. 「**この質問の名前の指定 (What do you want to name this question)**」フィールドで、質問の名前を入力します。
5. この質問に関連付ける重要度のレベルを「**重要度因子 (Importance Factor)**」リストから選択します。
6. 「**質問に含めるテストの指定 (Which tests do you want to include in your question)**」フィールドで、「**CIS ベンチマークの使用によるアセットの保存済み検索でアセットのコンプライアンスをテスト (test compliance of assets in asset saved searches with CIS benchmarks)**」テストの横にある追加 (+) アイコンを選択します。

   必要な場合、このテストを複数回選択します。

7. テストのパラメーターを「**アセットの検出 (Find Assets that)**」フィールドで構成します。

   各パラメーターをクリックして、質問について選択可能なオプションを表示します。必要な場合、複数のアセットの保存済み検索と複数のチェックリストをこのテストで指定します。

8. グループ域で、関係するチェック・ボックスをクリックし、グループ・メンバーシップをこの質問に割り当てます。

   アセット・コンプライアンスの質問は、コンプライアンス・ダッシュボードまたはレポートに含めるためにグループに割り当てておく必要があります。

9. 「**質問の保存 (Save Question)**」をクリックします。

次のタスク

作成した質問にベンチマーク・プロファイルを関連付け、質問の結果をモニターします。

関連概念:

45 ページの『重要度係数』
重要度係数は、リスク・スコアの計算、および質問に対して返される結果の数の定義に使用されます。

61 ページの『質問のグループ化』
選択した基準に応じて質問をグループ化して表示できます。

関連タスク:

50 ページの『アセット・コンプライアンスの質問のモニター』
アセット・コンプライアンスの質問は、CIS スキャン・プロファイルを選択してモニターします。 CIS ベンチマーク・スキャンは、アセットに対して実行します。

アセット・コンプライアンスの質問のモニター

アセット・コンプライアンスの質問は、CIS スキャン・プロファイルを選択してモニターします。 CIS ベンチマーク・スキャンは、アセットに対して実行します。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**ポリシー・モニター**」をクリックします。
3. 「**質問**」ペインで、モニターするアセット・コンプライアンスの質問を選択します。
4. 「**モニター**」をクリックして、「結果のモニター」ウィンドウを開きます。
5. ベンチマーク・プロファイルを「**この質問に関連付けるベンチマーク・プロファイル (Which benchmark profile to associate with this question?)**」リストから選択します。

   選択されたベンチマーク・スキャン・プロファイルは、ドメインに関連付けられている QRadar Vulnerability Manager スキャナーを使用します。ドメイン・ネームは、「**ベンチマーク・プロファイルの詳細 (Benchmark Profile Details)**」領域に表示されます。ドメイン管理について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
6. 「**この質問/シミュレーションのモニター結果機能を有効にする (Enable the monitor results function for this question/simulation)**」チェック・ボックスを選択します。
7. 「**モニターの保存 (Save Monitor)**」をクリックします。

   モニターは、ベンチマーク・スキャン・プロファイルの作成時に「**スキャン時期 (When To Scan)**」タブで設定したスキャン開始時刻に開始されます。

関連タスク:

49 ページの『コンプライアンス・ベンチマークの編集』
デフォルトの CIS ベンチマークにテストを追加したりテストを削除したりするには、IBM Security QRadar Risk Manager のコンプライアンス・ベンチマーク・エディターを使用します。

48 ページの『アセット・コンプライアンスの質問の作成』
CIS ベンチマーク・テストで不合格となるネットワーク内のアセットを検索するアセット・コンプライアンスの質問をポリシー・モニター内で作成します。

スキャン結果の表示

「スキャン結果」ページには、スキャン・プロファイルの実行によって生成された結果のサマリー・リストが表示されます。

このタスクについて

「スキャン結果」ページには、以下の情報が表示されます。

表 12. スキャン結果リスト・パラメーター

パラメーター	説明
プロファイル	スキャン・プロファイルの名前。「**プロファイル**」の上にマウスを移動すると、スキャン・プロファイルおよびスキャンの状況に関する情報が表示されます。
スケジュール (Schedule)	スキャン・プロファイルに適用される実行スケジュール。手動スキャンを開始した場合は、「**手動**」が表示されます。
スコア	スキャンの平均共通脆弱性評価システム (CVSS) スコア。このスコアは、脆弱性の優先順位付けに役立ちます。
ホスト数	スキャン・プロファイルが実行されたときに検出およびスキャンされたホストの数。 「**ホスト**」列のリンクをクリックすると、スキャンされたホストの脆弱性データが表示されます。
脆弱性	スキャンによって検出されたさまざまなタイプの脆弱性の数。 「**脆弱性**」列のリンクをクリックすると、すべての固有の脆弱性が表示されます。
脆弱性インスタンス	スキャンによって検出された脆弱性の数。
オープン・サービス	スキャンによって検出された固有のオープン・サービスの数。固有のオープン・サービスは、単一のオープン・サービスとしてカウントされます。 「**オープン・サービス**」列のリンクをクリックすると、オープン・サービス別に分類された脆弱性が表示されます。

表 12. スキャン結果リスト・パラメーター (続き)

パラメーター	説明
状況 (Status)	スキャン・プロファイルの状況。オプションは以下のとおりです。 • 停止 (Stopped) - この状況は、スキャンが正常に完了したか、スキャンがキャンセルされた場合に表示されます。 • 実行中 - スキャンが実行中です。 • 一時停止 - スキャンが一時停止中です。 • 未開始 (Not Started) - スキャンが開始されていません。
進行	スキャンの進行状況を指定します。 スキャンの実行中に、進行状況表示バーの上にマウスを移動すると、スキャンの状況に関する情報が表示されます。
開始日付/時刻 (Start Date/Time)	スキャン・プロファイルの実行が開始された日時。
Duration	スキャンが完了するまでにかかった時間を表示します。

手順

1. 「**脆弱性**」タブをクリックします。
2. ナビゲーション・ペインで、「**スキャン結果**」をクリックします。

Check Point デバイスのファイアウォール・ルール・イベント・カウントのモニター

IBM Security QRadar Risk Manager では、Check Point SMS と統合することにより、Check Point デバイスのファイアウォール・ルール・イベントのカウントをモニターできます。QRadar Risk Manager でこれらのルールによる対話を表示し、ルールのレポートを使用してネットワークのルール・ポリシーの有効性を管理できます。

以下の図では、QRadar が Check Point Firewall デバイスから SMS を介してルール・イベント・ログを受信し、処理しています。

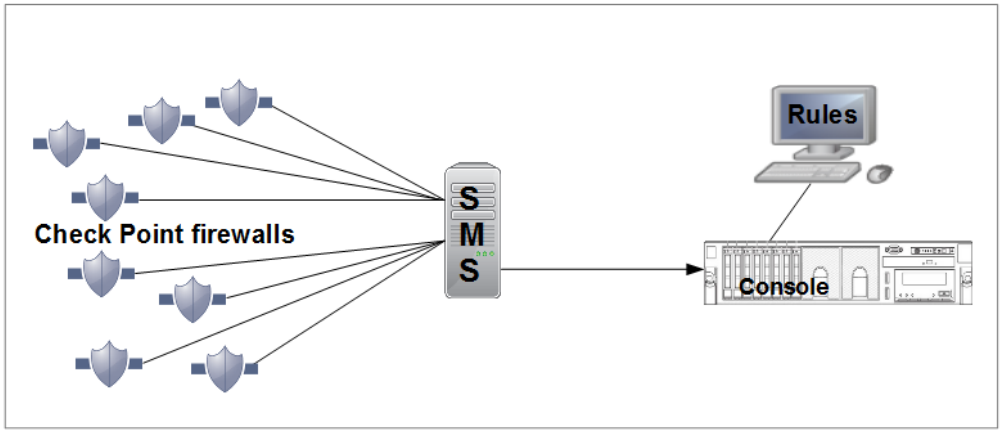

図 1. Check Point ルールのカウント

シナリオ - Check Point ファイアウォール・ルールのモニターを QRadar に実装する

ネットワーク・システム管理者が、Check Point を使用してネットワーク・セキュリティー・ポリシーを実装している組織で、ネットワーク・セキュリティーを担当しています。ネットワークには複数の Check Point ファイアウォールがあり、Check Point Security Management Server (SMS) から管理されています。

管理者は、ルール実装の詳細を確認するために、ルールの使用状況についてのレポートを毎日確認します。

QRadar が Check Point ファイアウォール・デバイスからルール・イベント・ログを受信するように、Check Point SMS と QRadar との間の接続を構成する必要があります。QRadar は、このルール・イベント・ログ情報を処理し、Check Point ファイアウォールで管理されているすべてのデバイスのルール・イベント情報を表示します。QRadar ルール・テーブルのイベント数をモニターしてファイアウォールの使用状況と有効性を分析してから、微調整を行って最適なパフォーマンスを得ることができます。

ルールの情報を使用して、以下のタスクを実行します。

- 頻度使用が最も高いルールと最も低いルールを確認する。
- トリガーされる頻度が少ないルールの実用性を評価する。
- ネットワーク・アクセスを必要以上にブロックしている可能性があるルールを確認する。
- 過剰にトリガーされて、ネットワーク帯域幅に負荷をかけているルールを確認する。
- 詳細なイベントを表示する。
- レポートをスケジュールする。

始める前に、Fix Central から最新のアダプター・バンドルをダウンロードして、QRadar の管理対象ホストにインストールします。

以下の手順に従って、ルールのカウントをセットアップします。

1. Check Point SmartDashboard で OPSEC アプリケーションを構成します。

2. QRadar でログ・ソースを作成します。
3. QRadar Risk Manager で構成ソース管理 (CSM) を構成します。構成ソース管理で、デバイスをディスカバーしてバックアップします。
4. 構成を完了してルールのカウントを確認します。

SmartDashboard での OPSEC アプリケーションの構成

Check Point SmartDashboard で 2 つの OPSEC アプリケーションを作成して構成します。これにより、Check Point と IBM Security QRadar の間でのログ・ファイルの転送が容易になります。

このタスクについて

2 つの OPSEC (Open Platform for Security) アプリケーションを作成します。1 つはクライアント・エンティティー・プロパティーが CPMI (Check Point 管理インターフェース) である QRadar Risk Manager 用のアプリケーションで、もう 1 つはクライアント・エンティティー・プロパティーが LEA (ログ・エクスポート API) である QRadar Risk Manager ログ・ソース用のアプリケーションです。

手順

1. ツールバーの「**管理 (Manage)**」メニューから、「**サーバーおよび OPSEC アプリケーション (Servers and OPSEC Applications)**」をクリックします。
2. 「**新規**」 > 「**OPSEC アプリケーション (OPSEC Application)**」をクリックします。
3. 「**名前**」フィールドに、アプリケーションの名前を入力します。
4. 「**ホスト**」リストから、ホストを選択するか、または「**新規**」をクリックしてホストを追加します。
5. 「**クライアント・エンティティー (Client Entities)**」で、「**CPMI**」チェック・ボックスを選択します。

   このオプションは QRadar Risk Manager 構成ソース管理 (Configuration Source Management) (CSM) のために必要です。
6. 「**通信 (Communication)**」をクリックします。
7. 「**ワンタイム・パスワード (One-time password)**」フィールドにパスワードを入力し、さらにパスワードを確認します。

   このパスワードはセットアップ中に何度か使用され、QRadar が Check Point からのセキュリティー証明書を使用できるように再使用する必要があります。
8. 「**初期化 (Initalize)**」をクリックします。

   「**トラスト状態 (Trust state)**」が **Initialized but trust not established** に変わります。
9. 「**閉じる**」をクリックします。
10. 「セキュアな内部通信 (Secure Internal Communication)」セクションの「**DN**」フィールドにデータを取り込むために、「**OK**」をクリックします。
11. データが取り込まれた「**DN**」フィールドを表示するために、「OPSEC アプリケーション (OPSEC Application)」を選択して、「**編集**」をクリックします。

「**DN**」フィールドにデータが取り込まれています。この情報は、QRadar でログ・ソースおよび構成ソース管理をセットアップする際に、「**アプリケーション・オブジェクト SIC 属性 (SIC 名) (Application Object SIC Attribute (SIC Name))**」および「**SIC 属性 (SIC 名) (SIC Attribute (SIC Name))**」で使用されます。

12. ログ・ソースで使用する 2 つ目の OPSEC アプリケーションを作成します。

    最初の OPSEC アプリケーションを作成するためのステップ 1 から 11 に従います。ただし、以下の 2 つの違いがあります。

    - ステップ 3 の「**名前**」フィールドで、最初の OPSEC アプリケーションとは異なる名前を使用します。
    - ステップ 5 の「**クライアント・エンティティー (Client Entities)**」で、「**LEA**」チェック・ボックスを選択します。

    「**トラスト状態 (Trust state)**」に `Initialized but trust not established` と表示されていることを確認します。

    ヒント: パスワードの混同を避けるために、この OPSEC アプリケーションでも同じワンタイム・パスワードを使用します。

13. SmartDashboard で、メインの SmartDashboard ウィンドウに戻るまですべてのウィンドウを閉じます。
14. ツールバーの「**ポリシー (Policy)**」メニューから、「**インストール (Install)**」をクリックします。
15. 「**選択したすべてのゲートウェイにインストール (失敗した場合は同じバージョンのゲートウェイにインストールしない) (Install on all selected gateways, if it fails do not install on gateways of the same version)**」をクリックします。

次のタスク

次のステップは QRadar でのログ・ソースの構成です。

ログ・ソースの構成

IBM Security QRadar でログ・ソースを構成して、Check Point から証明書を取得し、ログ情報を受信します。

手順

1. QRadar にログオンします。
2. 「**管理**」タブをクリックします。
3. ナビゲーション・メニューで、「**データ・ソース**」をクリックします。

   「データ・ソース」ペインが表示されます。

4. 「**ログ・ソース**」アイコンをクリックします。
5. 「**追加**」をクリックします。
6. 以下の値を構成します。

表 13. Check Point ログ・ソースのパラメーター

パラメーター	説明
ログ・ソース名	ログ・ソースの ID。
ログ・ソースの説明	この説明はオプションです。
ログ・ソース・タイプ	「**Check Point FireWall-1**」を選択します。
プロトコル構成	「**OPSEC/LEA**」を選択します。
ログ・ソース ID	SMS の IP アドレス
サーバー IP (Server IP)	SMS の IP アドレスを入力します。
サーバー・ポート	ポート 18184 を使用します。
ログ・ソースにサーバー IP を使用 (Use Server IP for Log Source)	このチェック・ボックスは選択しないでください。
統計レポートの間隔 (Statistics Report Interval)	デフォルトの 600。
認証タイプ	リストから「**sslca**」を選択します。
OPSEC アプリケーション・オブジェクト SIC 属性 (SIC 名) (OPSEC Application Object SIC Attribute (SIC Name))	Check Point の SmartDashboard で、「**管理 (Manage)**」 > 「**サーバーおよび OPSEC アプリケーション (Servers and OPSEC Applications)**」をクリックし、クライアント・エンティティー・プロパティーが LEA である OPSEC アプリケーションを選択します。 「**編集**」をクリックし、「**DN**」フィールドのエントリーをコピーして「**OPSEC アプリケーション・オブジェクト SIC 属性 (OPSEC Application Object SIC Attribute (SIC Name)**」フィールドに貼り付けます。

表 13. Check Point ログ・ソースのパラメーター (続き)

パラメーター	説明

ログ・ソース SIC 属性 (エンティティー SIC 名) (Log Source SIC Attribute (Entity SIC Name))	「**OPSEC アプリケーション・オブジェクト SIC 属性 (SIC 名) (OPSEC Application Object SIC Attribute (SIC Name)**」フィールドに貼り付けたエントリーを使用し、`CN= property value` からテキストを削除して、次のように編集します。
	
	`CN=` プロパティー値に対して、`cp_mgmt_ <hostname >` を使用します。
	
	ここで、*<hostname>* は「OPSEC アプリケーション・プロパティー (OPSEC Application Properties)」ウィンドウの「**ホスト**」名です。
	
	エンティティー SIC 名を作成するために使用される、OPSEC アプリケーション DN (OPSEC Application DN) と OPSEC アプリケーション・ホスト (OPSEC Application Host) の例を以下に示します。
	
	OPSEC アプリケーション DN (OPSEC Application DN):
	`CN=cpsmsxxx,O=svxxx-CPSMS..bsaobx`
	
	OPSEC アプリケーション・ホスト (OPSEC Application Host):
	`Srvxxx-SMS`
	
	OPSEC アプリケーション DN (OPSEC Application DN) と OPSEC アプリケーション・ホスト (OPSEC Application Host) のテキストを使用して、以下のように「**エンティティー SIC 名 (Entity SIC Name)**」を構成します。
	
	`CN=cp_mgmt_Srvxxx-SMS,O=svxxx-CPSMS..bsaobx`
	
	この構成の「**エンティティー SIC 名 (Entity SIC Name)**」は、管理サーバーへのゲートウェイのセットアップに基づいています。SMS アドレスがゲートウェイとして使用されない場合は、「**エンティティー SIC 名 (Entity SIC Name)**」に管理サーバー構成を使用します。これは次のテキストのように表現されます。
	
	`CN=cp_mgmt,O=<take_O_value_from_DN_field>`

証明書の指定 (Specify Certificate)	このチェック・ボックスは選択しないでください。
認証局 IP (Certificate Authority IP)	SMS の IP アドレスを入力します。
証明パスワードのプル (Pull Certificate Password)	「OPSEC アプリケーション・プロパティー (OPSEC Applications Properties)」の「通信 (Communication)」ウィンドウの「**ワンタイム・パスワード (One-time password)**」フィールドに指定したパスワード。
OPSEC アプリケーション (OPSEC Application)	「OPSEC アプリケーション・プロパティー (OPSEC Applications Properties)」の「**名前**」フィールドに指定した名前。
有効	ログ・ソースを有効にするにはこのチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。

表 13. Check Point ログ・ソースのパラメーター (続き)

パラメーター	説明
信頼性	範囲は 0 から 10 です。送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	リストから、ログ・ソースのターゲットとして使用する「**ターゲット・イベント・コレクター**」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにします。デフォルトでは、自動的にディスカバーされたログ・ソースは、QRadar の「システム設定」プロパティーから「**イベントの統合**」リストの値を継承します。ログ・ソースを作成する際、または既存の構成を編集する際に、ログ・ソースごとにこのオプションを構成してデフォルト値をオーバーライドすることができます。
イベント・ペイロードの保管	ログ・ソースでイベント・ペイロード情報を保管できるようにします。デフォルトでは、自動的にディスカバーされたログ・ソースは、QRadar の「システム設定」プロパティーから「**イベント・ペイロードの保管**」リストの値を継承します。ログ・ソースを作成する際、または既存の構成を編集する際に、ログ・ソースごとにこのオプションを構成してデフォルト値をオーバーライドすることができます。

7. 「**保存**」をクリックします。
8. 「**管理**」タブで「**変更のデプロイ**」をクリックします。

   変更が自動的に実装されることが分かった場合でも、「**変更のデプロイ**」をクリックすることをお勧めします。

   クライアント・エンティティー・プロパティーが LEA である OPSEC アプリケーションに対してトラストが確立されたことを確認するために、「OPSEC アプリケーション・プロパティー (OPSEC Application Properties)」の「通信 (Communication)」ウィンドウの「**トラスト状態 (Trust State)**」を表示します。

   ログ・ソースの構成が完了しました。

   ログ・ソースの構成について詳しくは、*IBM Security QRadar Managing Log Sources Guide* を参照してください。

Check Point と IBM Security QRadar の間のセキュアな通信の確立

Check Point SMS に接続するための構成ソース管理を IBM Security QRadar に構成します。SmartDashboard から OPSEC アプリケーションの詳細を追加し、Check Point からセキュリティー証明書を要求します。

このタスクについて

「構成ソース管理 (Configuration Source Management)」で OPSEC アプリケーションの詳細を構成し、証明書の交換をセットアップします。構成が完了した後、「構成ソース管理 (Configuration Source Management)」を使用して、新しいエントリーをディスカバーします。

手順

1. QRadar に管理者としてログインします。
2. 「**管理**」タブをクリックします。
3. ナビゲーション・メニューで、「**プラグイン**」をクリックするか、スクロールダウンして「**構成ソース管理 (Configuration Source Management)**」アイコンを見つけます。
4. 「**構成ソース管理 (Configuration Source Management)**」アイコンをクリックします。
5. ナビゲーション・メニューで「**資格情報 (Credentials)**」をクリックします。
6. 「ネットワーク・グループ (Network Groups)」ペインで、**(+)** 記号をクリックします。
7. ネットワーク・グループの名前を入力します。
8. 「**アドレスの追加 (IP、CIDR、ワイルドカード、または範囲) (Add address (IP, CIDR, Wildcard, or Range))**」フィールドに、SMS の IP アドレスを入力します。
9. **(+)** をクリックして IP アドレスを追加します。
10. SMS SmartDashboard のユーザー名とパスワードを入力します。

    OPSEC の各フィールドを構成するために、クライアント・エンティティー用の「**CPMI**」チェック・ボックスを選択した SmartDashboard の「OPSEC アプリケーション・プロパティー (OPSEC Application Properties)」ウィンドウの情報を使用します。
11. 「**DN**」フィールドの情報をコピーして、「**OPSEC エンティティー SIC 名 (OPSEC Entity SIC Name)**」フィールドに貼り付けます。
12. 「**OPSEC エンティティー SIC 名 (OPSEC Entity SIC Name)**」に貼り付けた項目を編集し、CN= のプロパティー値を cp_mgmt_<*hostname*> で置き換えます。

    ここで、<*hostname*> は OPSEC アプリケーションの「**ホスト**」フィールドに使用される**ホスト**名です。

    エンティティー SIC 名を作成するために使用される、OPSEC アプリケーション DN (OPSEC Application DN) と OPSEC アプリケーション・ホスト (OPSEC Application Host) の例を以下に示します。

    - OPSEC アプリケーション DN (OPSEC Application DN): `CN=cpsmsxxx,O=svxxx-CPSMS..bsaobx`
    - OPSEC アプリケーション・ホスト (OPSEC Application Host): `Srvxxx-SMS`

    OPSEC アプリケーション DN (OPSEC Application DN) と OPSEC アプリケーション・ホスト (OPSEC Application Host) のテキストを使用して、以下のように「**エンティティー SIC 名 (Entity SIC Name)**」を構成します。

    「**エンティティー SIC 名 (Entity SIC Name)**」は `CN=cp_mgmt_Srvxxx-SMS,O=svxxx-CPSMS..bsaobx` となります。

この構成の「**エンティティー SIC 名 (Entity SIC Name)**」は、管理サーバーへのゲートウェイのセットアップに基づいています。SMS の IP アドレスがゲートウェイとして使用されていない場合は、以下の表の管理サーバーの構成を使用してください。

表 14. エンティティー SIC 名の形式

タイプ	名前
管理サーバー	CN=cp_mgmt,O=*<take_O_value_from_DN_field>*
管理サーバーへのゲートウェイ	CN=cp_mgmt_*<gateway_hostname>*,O=*<take_O_value from_DN_field>*

13. 「**DN**」フィールドから項目をコピーし、この情報を「**OPSEC アプリケーション・オブジェクト SIC 名 (OPSEC Application Object SIC Name)**」フィールドに貼り付けます。
14. 「**証明書の取得 (Get Certificate)**」をクリックします。
15. 「**認証局 IP (Certificate Authority IP)**」フィールドに SMS の IP アドレスを入力します。
16. 「**証明書パスワードのプル (Pull Certificate Password)**」フィールドにワンタイム・パスワードを入力します。 このワンタイム・パスワードは、クライアント・エンティティー用の「**CPMI**」チェック・ボックスを選択した SmartDashboard の「OPSEC アプリケーション・プロパティー (OPSEC Application Properties)」の「通信 (Communication)」ウィンドウからのものです。
17. 「**OK**」をクリックします。

    正常に完了すると、「**OPSEC SSL 証明書 (OPSEC SSL Certificate)**」フィールドにデータが取り込まれ、グレー表示になります。

    「OPSEC アプリケーション・プロパティー (OPSEC Application Properties)」の「通信 (Communication)」ウィンドウ内の「**トラスト状態 (Trust State)**」プロパティーが **Trust established** に変化することを確認します。

    これで資格情報がセットアップされ、ディスカバリーを実行できるようになりました。
18. ナビゲーション・メニューで、「**Check Point SMS からディスカバー (Discover From Check Point SMS)**」をクリックします。
19. 「**CPSMS IP アドレス (CPSMS IP Address)**」フィールドに、SMS の IP アドレスを入力します。

Check Point のルール・カウントの初期化

IBM Security QRadar および Check Point の最終構成を完了して構成を統合し、QRadar でルール・カウントを使用できるようにします。

このタスクについて

トラストが確立され、ポリシーが更新されると、QRadar でルール・カウントを表示できるようになります。QRadar Risk Manager では、カウントを処理するためにおよそ 1 時間が必要となります。

手順

1. QRadar で、「**リスク**」 > 「**構成モニター (Configuration Monitor)**」をクリックします。
2. Check Point デバイスをダブルクリックしてルール・カウントを表示します。
   - 「**ログ・ソース**」列を見て、ログ・ソースが自動マッピングになっていることを確認します。
   - ルール・テーブルの「**イベント数**」列を見つけます。

ポリシー・モニターの質問

ネットワーク・デバイスまたはネットワーク・デバイス上のルールに存在するリスクを識別するためのテストの質問を定義できます。

ポリシー・モニター・テストの汎用パラメーターとテスト固有のパラメーター

パラメーターは、ポリシー・モニター・テストごとに構成します。構成可能なパラメーターは、太字になっていて、下線が付いています。パラメーターをクリックすると、質問に使用可能なオプションが表示されます。

ポリシー・モニター・テストで使用するパラメーターには、汎用パラメーターとテスト固有のパラメーターの 2 つのタイプがあります。汎用パラメーターには、テストをカスタマイズするための 2 つ以上のオプションが用意されています。汎用パラメーターをクリックすると、使用可能な選択項目が切り替わります。テスト固有のパラメーターには、ユーザーの入力が必要です。テスト固有のパラメーターをクリックして、情報を指定します。

例えば、「**宛先リモート・ネットワーク・ロケーションへの通信が受け入れられたことがある (have accepted communication to destination remote network locations)**」というアセット・テストには、2 つの汎用パラメーターと 1 つのテスト固有のパラメーターが含まれます。汎用パラメーター「**受け入れたことがある (have accepted)**」をクリックして、「**受け入れたことがある (have accepted)**」または「**拒否したことがある (have rejected)**」のいずれかを選択します。汎用パラメーター「**宛先 (to destination)**」をクリックして、「**宛先 (to destination)**」または「**送信元 (from source)**」のいずれかを選択します。テスト固有のパラメーター「**リモート・ネットワーク・ロケーション (remote network locations)**」をクリックして、アセット・テストのリモート・ロケーションを追加します。

アセット・テストの質問

アセットの質問を使用して、定義済みポリシーに違反している、または環境にリスクをもたらしている、ネットワーク上のアセットを識別します。

アセット・テストの質問は、実際の通信または可能な通信のいずれかの通信タイプに分類されます。どちらの通信タイプも、寄与テストと制限テストを使用します。

実際の通信テストには、接続を使用して通信が検出されたアセットが含まれます。可能な通信の質問を使用すると、通信が検出されたかどうかに関係なく、アセットで特定の通信が可能であるかどうかを検討できます。

寄与テストの質問は基本となるテストの質問であり、テストしようとしている実際の通信のタイプを定義します。

制限テストの質問は寄与テストによる結果を制限し、特定の違反を対象に、実際の通信をさらにフィルタリングします。

制限テストを使用する場合、その制限テストの方向は寄与テストと同じ方向に従っていなければなりません。インバウンド方向とアウトバウンド方向を混用する制限テストを使用できるのは、2 つのポイント (2 つのネットワークまたは 2 つの IP アドレスなど) の間にあるアセットを特定しようとする場合です。

インバウンドとは、該当するアセットが宛先となっている接続をフィルタリングするテストを意味します。アウトバウンドとは、該当するアセットが送信元となっている接続をフィルタリングするテストを意味します。

デバイス/ルール・テストの質問

デバイスおよびルールを使用して、定義済みのポリシーに違反していて、環境にリストをもたらす可能性のあるデバイスのルールを識別します。

デバイス・ルールの質問の詳細なリストについては、デバイス/ルール・テストの質問を参照してください。

実際の通信のテストの寄与質問

アセットに対する実際の通信のテストには、寄与質問とパラメーターがあります。これらの質問およびパラメーターは、ポリシー・モニター・テストの作成時に選択します。

「have not (否定)」条件をテストに適用した場合、否定条件はテストするパラメーターに関連付けられます。

例えば、テストを「**宛先ネットワークへの通信が受け入れられたことがない (have not accepted communication to destination networks)**」として構成すると、このテストでは、構成済みのネットワーク以外のネットワークへの通信が受け入れられたアセットを検出します。別の例として、テストを「インターネットへの通信が受け入れられたことがない (have not accepted communication to the Internet)」として構成すると、テストでは、インターネット以外への通信が受け入れられたアセット、またはインターネット以外からの通信を受け入れたアセットを検出します。

以下の表に、実際の通信のテストの寄与質問パラメーターをリストして説明します。

表 15. 実際の通信のテストにおける寄与質問パラメーター

テスト名	説明
任意の宛先への通信が受け入れられたことがある (have accepted communication to any destination)	任意の構成済みネットワークとの通信を行うアセットを検出します。 このテストでは、質問に通信の開始点または終点を定義できます。 例えば、DMZ からの通信を受け入れたアセットを識別するには、テストを以下のように構成します。 任意の送信元からの通信を受け入れたことがある (have accepted communication from any source) このテストを使用して、ポリシーに従っていない通信を検出できます。
宛先ネットワークへの通信が受け入れられたことがある (have accepted communication to destination networks)	指定したネットワークとの通信を行うアセットを検出します。 このテストでは、質問に通信の開始点または終点を定義できます。 例えば、DMZ と通信したアセットを識別するには、テストを以下のように構成します。 送信元 <networks> からの通信を受け入れたことがある (have accepted communication from source <networks>) このテストを使用して、ポリシーに従っていない通信を検出できます。
宛先 IP アドレスへの通信が受け入れられたことがある (have accepted communication to destination IP addresses)	指定した IP アドレスとの通信を行うアセットを検出します。 このテストでは、IP アドレスを指定することも、CIDR アドレスを指定することもできます。 例えば、特定のコンプライアンス・サーバーへの通信を行ったことがあるすべてのアセットを識別するには、テストを以下のように構成します。 宛先 <compliance server IP address> への通信が受け入れられたことがある (have accepted communications to destination <compliance server IP address>)

表 15. 実際の通信のテストにおける寄与質問パラメーター (続き)

テスト名	説明
宛先アセット・ビルディング・ブロックへの通信が受け入れられたことがある (have accepted communication to destination asset building blocks)	指定したアセット・ビルディング・ブロックとの通信を行うアセットを検出します。このテストでは、QRadar ルール・ウィザードで定義されたビルディング・ブロックを照会で再利用できます。 ルール、アセット、ビルディング・ブロックについて詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
宛先アセットの保存済み検索への通信が受け入れられたことがある (have accepted communication to destination asset saved searches)	指定した保存済み検索によって返されたアセットとの通信を行うアセットを検出します。 アセット検索の作成および保存については、「*IBM Security QRadar SIEM ユーザーズ・ガイド*」を参照してください。
宛先リファレンス・セットへの通信が受け入れられたことがある (have accepted communication to destination reference sets)	定義済みリファレンス・セットとの通信を行うアセットを検出します。
宛先リモート・ネットワーク・ロケーションへの通信が受け入れられたことがある (have accepted communication to destination remote network locations)	リモート・ネットワークとして定義されたネットワークと通信したことがあるアセットを検出します。 例えば、このテストでは、ボットネットやその他の疑わしいインターネット・アドレス・スペースへの通信を行ったことがあるホストを識別できます。
地理上の宛先ネットワーク・ロケーションへの通信が受け入れられたことがある (have accepted communication to destination geographic network locations)	地理上のネットワークとして定義されたネットワークと通信したことがあるアセットを検出します。 例えば、このテストでは、業務を行っていない国との通信を試行したアセットを検出できます。
インターネットへの通信が受け入れられたことがある (have accepted communication to the Internet)	送信元または宛先とインターネットとの間の通信を検出します。
以下の脆弱性のいずれかの影響を受けやすい (are susceptible to one of the following vulnerabilities)	特定の脆弱性を検出します。 特定のタイプの脆弱性を検出するには、テスト「**以下の分類のいずれかに属する脆弱性の影響を受けやすい (are susceptible to vulnerabilities with one of the following classifications)**」を使用します。 OSVDB ID、CVE ID、Bugtraq ID、またはタイトルで脆弱性を検索できます。

表 15. 実際の通信のテストにおける寄与質問パラメーター (続き)

テスト名	説明
以下の分類のいずれかに属する脆弱性の影響を受けやすい (are susceptible to vulnerabilities with one of the following classifications)	脆弱性を 1 つ以上の脆弱性分類に関連付けることができます。このテストは、指定された分類に属する脆弱性が含まれるすべてのアセットをフィルタリングします。 「**分類**」パラメーターを構成して、このテストを適用する脆弱性分類を指定します。 例えば、脆弱性分類として、入力操作 (Input Manipulation) やサービス妨害 (Denial of Service) などがあります。
CVSS スコアが 5 より大きい脆弱性の影響を受けやすい (are susceptible to vulnerabilities with CVSS score greater than 5)	共通脆弱性評価システム (CVSS) の値は、脆弱性の重大度を評価するための業界標準です。CVSS は、基本、一時的、環境の 3 つのメトリック・グループで構成されます。これらのメトリックを使用することで、CVSS では脆弱性の基本的特性を定義して伝えることができます。 このテストは、ユーザーが指定した CVSS スコアの脆弱性が含まれる、ネットワーク内のアセットをフィルタリングします。
指定の日付後に公開された脆弱性の影響を受けやすい (are susceptible to vulnerabilities disclosed after specified date)	構成された日付の後、前、またはその当日に公開された脆弱性を持つ、ネットワーク内のアセットを検出します。
以下のポートのいずれかで脆弱性の影響を受けやすい (are susceptible to vulnerabilities on one of the following ports)	構成されたポートに関連付けられた脆弱性を持つ、ネットワーク内のアセットを検出します。 「**ポート**」パラメーターを構成して、このテストの対象とするポートを識別します。
名前、ベンダー、バージョン、またはサービスに以下のいずれかのテキスト項目が含まれている、脆弱性の影響を受けやすい (are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries)	1 つ以上のテキスト項目に基づき、アセット名、ベンダー、バージョン、またはサービスと一致する、ネットワーク内の脆弱性を持つアセットをフィルタリングします。 「**テキスト項目 (text entries)**」パラメーターを構成して、このテストの対象とするアセット名、ベンダー、バージョン、またはサービスを指定します。
名前、ベンダー、バージョン、またはサービスに以下のいずれかの正規表現が含まれている、脆弱性の影響を受けやすい (are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions)	1 つ以上の正規表現に基づき、アセット名、ベンダー、バージョン、またはサービスと一致する、ネットワーク内の脆弱性を持つアセットをフィルタリングします。 「**正規表現**」パラメーターを構成して、このテストの対象とするアセット名、ベンダー、バージョン、またはサービスを指定します。

表 15. 実際の通信のテストにおける寄与質問パラメーター (続き)

テスト名	説明
脆弱性の保存済み検索内に含まれる脆弱性の影響を受けやすい (are susceptible to vulnerabilities contained in vulnerability saved searches)	IBM Security QRadar Vulnerability Manager で作成された保存済み検索に関連付けられたリスクを検出します。

非推奨となった寄与テストの質問

別のテストに置き換えられた寄与テストの質問は、ポリシー・モニターで非表示になります。

ポリシー・モニターで非表示になるテストは以下のとおりです。

- 脆弱性の影響を受けやすいアセット (assets that are susceptible to vulnerabilities)
- 以下のサービスからの脆弱性の影響を受けやすいアセット (assets that are susceptible to vulnerabilities from the following services)

上記の寄与テストは、他のテストに置き換えられました。

実際の通信テストの制限質問

アセットの実際の通信テストには、制限の質問とパラメーターが含まれます。これらの質問およびパラメーターは、ポリシー・モニター・テストの作成時に選択できます。

除外条件をテストに適用する場合、除外条件はプロトコル・パラメーターに適用されます。

例えば、このテストを「**以下のプロトコルを除外する (exclude the following protocols)**」ように構成すると、テストでは、除外対象のプロトコルを使用していないアセットのみが返されます。

以下の表に、実際の通信テストの制限質問パラメーターをリストして説明します。

表 16. 実際の通信テストの制限質問パラメーター

テスト名	説明
以下のプロトコルのみを含める (include only the following protocols)	指定したプロトコルを含むか、それらのプロトコルを除外する寄与テストからのアセットをフィルターに掛けます。 このテストを選択できるのは、この質問にアセットの寄与テストが追加されている場合のみです。
以下のインバウンド・ポートのみを含める (include only the following inbound ports)	指定したポートのみを含むか、それらのポートを除外する寄与テストからのアセットをフィルターに掛けます。 このテストを選択できるのは、この質問にアセットの寄与テストが追加されている場合のみです。

表 16. 実際の通信テストの制限質問パラメーター (続き)

テスト名	説明
以下のインバウンド・アプリケーションのみを含める (include only the following inbound applications)	インバウンドまたはアウトバウンド・アプリケーションのみを含むか、それらのアプリケーションを除外する寄与テストの質問からのアセットをフィルターに掛けます。 このテストは、フロー・データだけが含まれる接続をフィルタリングします。
送信元のインバウンド・バイト数と宛先のアウトバウンド・バイト数の差が 10 パーセント未満の場合にのみ含める (include only if the source inbound and destination outbound bytes have a percentage difference less than 10)	アウトバウンド・バイト数に対するインバウンド・バイト数 (またはインバウンド・バイト数に対するアウトバウンド・バイト数) が特定の比率になっている通信に基づき、寄与テストの質問からのアセットをフィルターに掛けます。 このテストは、プロキシー・タイプの動作 (インバウンドとアウトバウンドが等しい) を示しているホストを検出するのに役立ちます。
インバウンド・フロー数とアウトバウンド・フロー数の差が 10 パーセント未満の場合にのみ含める (include only if the inbound and outbound flow count has a percentage difference less than 10)	アウトバウンド・フロー数に対するインバウンド・フロー数 (またはインバウンド・フロー数に対するアウトバウンド・フロー数) が特定の比率になっている通信に基づき、寄与テストの質問からのアセットをフィルター掛けます。 フロー数が選択された場合、このテストはフロー・データが含まれる接続をフィルタリングします。 この制限テストには、送信元と宛先を指定する 2 つの寄与テストが必要です。以下のテストで、インバウンドとアウトバウンドのパーセンテージ差が 40 パーセントより大きい、2 つのポイントの間にあるアセットを判別するための一連の質問の概要を説明します。例えば、以下のようにします。 • **寄与テスト** - インターネットへの通信が受け入れられたことがある (have accepted communication to the Internet)。 • **寄与テスト** - かつ、インターネットからの通信を受け入れたことがある (and have accepted communication from the internet)。 • **制限テスト** - かつ、インバウンド・フロー数とアウトバウンド・フロー数の差が 40 パーセントより大きい場合にのみ含める (and include only if the inbound and outbound flow count has a percentage difference greater than 40)。

表 16. 実際の通信テストの制限質問パラメーター (続き)

テスト名	説明
時刻が開始時刻から終了時刻までの間である場合にのみ含める (include only if the time is between start time and end time inclusive)	特定の時刻範囲内に発生したネットワーク内の通信をフィルタリングします。これにより、ポリシーに従っていない通信を検出できます。例えば、企業ポリシーで FTP 通信を許可しているのが午前 1 時から午前 3 時までの間である場合、このテストによって、その時刻範囲外に FTP を使用して行われた通信試行を検出できます。
曜日が開始日から終了日までの間である場合にのみ含める (include only if the day of week is between start day and end day inclusive)	特定の時刻範囲内で発生したネットワーク通信に基づいて、寄与テストの質問からのアセットをフィルターに掛けます。これにより、ポリシーに従っていない通信を検出できます。
エクスプロイト可能な脆弱性の影響を受けやすい場合にのみ含める (include only if susceptible to vulnerabilities that are exploitable)	特定の脆弱性を検索する寄与テストの質問からのアセットをフィルターに掛け、結果をエクスプロイト可能なアセットに限定します。 この制限テストには構成可能なパラメーターは含まれませんが、寄与テスト「**以下の脆弱性のいずれかの影響を受けやすい (are susceptible to one of the following vulnerabilities)**」とともに使用されます。脆弱性パラメーターを含む、この要因となるルールは必須です。
以下のネットワークのみを含める (include only the following networks)	構成済みのネットワークを含むか、それらのネットワークを除外する寄与テストの質問からのアセットをフィルターに掛けます。
以下のアセット・ビルディング・ブロックのみを含める (include only the following asset building blocks)	構成済みのアセット・ビルディング・ブロックに関連付けられているか、それらのアセット・ビルディング・ブロックに関連付けられていない寄与テストの質問からのアセットをフィルターに掛けます。
以下のアセットの保存済み検索のみを含める (include only the following asset saved searches)	アセットの保存済み検索に関連付けられているか、それらの検索に関連付けられていない寄与テストの質問からのアセットをフィルターに掛けます。
以下のリファレンス・セットのみを含める (include only the following reference sets)	構成済みのリファレンス・セットを含むか、それらのリファレンス・セットを除外する寄与テストの質問からのアセットをフィルターに掛けます。
以下の IP アドレスのみを含める (include only the following IP addresses)	構成済みの IP アドレスに関連付けられているか、それらの IP アドレスに関連付けられていないアセットをフィルターに掛けます。

表 16. 実際の通信テストの制限質問パラメーター (続き)

テスト名	説明
オペレーティング・システムの Microsoft Windows Service Pack が 0 未満の場合にのみ含める (include only if the Microsoft Windows service pack for operating systems is below 0)	アセットをフィルターに掛けて、オペレーティング・システムの Microsoft Windows Service Pack のレベルが、自社のポリシーで規定するレベル未満であるかどうかを判別します。
Microsoft Windows のセキュリティー設定が 0 未満の場合にのみ含める (include only if the Microsoft Windows security setting is less than 0)	アセットをフィルターに掛けて、Microsoft Windows のセキュリティー設定が、自社のポリシーで規定するレベル未満であるかどうかを判別します。
Microsoft Windows サービスが状況に等しい場合にのみ含める (include only if the Microsoft Windows service equals status)	アセットをフィルターに掛けて、Microsoft Windows サービスが不明、ブート、カーネル、自動、デマンド、または無効であるかどうかを判別します。
Microsoft Windows の設定が正規表現に一致する場合にのみ含める (include only if the Microsoft Windows setting equals regular expressions)	アセットをフィルターに掛けて、Microsoft Windows の設定が指定の正規表現に一致するかどうかを判別します。

可能な通信のテストの寄与質問

アセットに対する、可能な通信のテストには、寄与質問とパラメーターがあります。これらの質問とパラメーターは、ポリシー・モニター・テストの作成時に選択できます。

以下の表に、可能な通信のテストの寄与質問パラメーターをリストして説明します。

表 17. 寄与テストにおける可能な通信の質問パラメーター

テスト名	説明
任意の宛先への通信が受け入れられたことがある (have accepted communication to any destination)	指定された送信元または宛先との通信が可能なアセットを検出します。例えば、重要なサーバーが任意の送信元からの通信を受信可能かどうかを判別するには、以下のようにテストを構成します。 任意の送信元からの通信を受け入れたことがある (have accepted communication from any source) 次に、制限テストを適用して、該当する重要なサーバーがポート 21 で任意の通信を受け入れたことがあるかどうかを返すようにすることができます。これにより、その重要なサーバーに対して、ポリシーに従っていない通信を検出できます。

表 17. 寄与テストにおける可能な通信の質問パラメーター (続き)

テスト名	説明
宛先ネットワークへの通信が受け入れられたことがある (have accepted communication to destination networks)	構成済みネットワークとの通信が可能なアセットを検出します。 このテストでは、質問に通信の開始点または終点を定義できます。 例えば、DMZ への通信が可能なアセットを識別するには、テストを以下のように構成します。 送信元 <networks> からの通信を受け入れたことがある (have accepted communication from source <networks>) このテストを使用して、ポリシーに従っていない通信を検出できます。
宛先 IP アドレスへの通信が受け入れられたことがある (have accepted communication to destination IP addresses)	構成済み IP アドレスとの通信が可能なアセットを検出します。このテストでは、可能な通信の対象として単一の IP アドレスを指定できます。例えば、特定のコンプライアンス・サーバーへの通信が可能なすべてのアセットを識別するには、テストを以下のように構成します。 宛先 <compliance server IP address> への通信が受け入れられたことがある (have accepted communications to destination <compliance server IP address>)
宛先アセット・ビルディング・ブロックへの通信が受け入れられたことがある (have accepted communication to destination asset building blocks)	ビルディング・ブロックを使用する構成済みアセットとの通信が可能なアセットを検出します。このテストでは、QRadar ルール・ウィザードで定義されたビルディング・ブロックを照会で再利用できます。例えば、保護されたアセットへの通信が可能なすべてのアセットを識別するには、テストを以下のように構成します。 宛先 `<BB:HostDefinition:Protected Assets>` への通信が受け入れられたことがある (have accepted communications to destination `<BB:HostDefinition:Protected Assets>`) ルールおよびビルディング・ブロックについて詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

表 17. 寄与テストにおける可能な通信の質問パラメーター (続き)

テスト名	説明
宛先アセットの保存済み検索への通信が受け入れられたことがある (have accepted communication to destination asset saved searches)	指定した保存済み検索によって返されたアセットへの通信が受け入れられたアセット、またはこのアセットからの通信を受け入れたアセットを検出します。 このテストを使用する前に、アセットの保存済み検索が存在している必要があります。アセット検索の作成および保存については、「*IBM Security QRadar SIEM ユーザーズ・ガイド*」を参照してください。
宛先リファレンス・セットへの通信が受け入れられたことがある (have accepted communication to destination reference sets)	送信元または宛先とリファレンス・セットとの間で通信が可能であるかどうかを検出します。
インターネットへの通信が受け入れられたことがある (have accepted communication to the Internet)	送信元または宛先とインターネットとの間で通信が可能かどうかを検出します。 インターネットへの通信トラフィック、またはインターネットからの通信トラフィックの方向を考慮するには、「**宛先**」または「**送信元 (from)**」パラメーターを指定します。
以下の脆弱性のいずれかの影響を受けやすい (are susceptible to one of the following vulnerabilities)	潜在的な特定の脆弱性を検出します。 特定のタイプの脆弱性を検出するには、テスト「**以下の分類のいずれかに属する脆弱性の影響を受けやすい (are susceptible to vulnerabilities with one of the following classifications)**」を使用します。 このテストを適用する脆弱性を指定します。脆弱性を検索するには、OSVDB ID、CVE ID、Bugtraq ID、またはタイトルを使用できます。
以下の分類のいずれかに属する脆弱性の影響を受けやすい (are susceptible to vulnerabilities with one of the following classifications)	脆弱性を、1 つ以上の脆弱性分類に関連付けることができます。このテストは、指定されたとおりに、共通脆弱性評価システム (CVSS) スコアを使用して、潜在的な脆弱性のあるすべてのアセットをフィルタリングします。 「分類」パラメーターを構成して、このテストを適用する脆弱性分類を指定します。

表 17. 寄与テストにおける可能な通信の質問パラメーター (続き)

テスト名	説明
CVSS スコアが 5 より大きい脆弱性の影響を受けやすい (are susceptible to vulnerabilities with CVSS score greater than 5)	共通脆弱性評価システム (CVSS) の値は、潜在的な脆弱性の重大度を評価するための業界標準です。CVSS は、基本、一時的、環境の 3 つのメトリック・グループで構成されます。これらのメトリックを使用することで、CVSS では脆弱性の基本的特性を定義して伝えることができます。 このテストは、構成済み CVSS 値を持つ、ネットワーク内のアセットをフィルタリングします。
指定の日付後に公開された脆弱性の影響を受けやすい (are susceptible to vulnerabilities disclosed after specified date)	構成された日付の後、前、またはその当日に公開された、潜在的な脆弱性のある、ネットワーク内のアセットをフィルタリングします。
以下のポートのいずれかで脆弱性の影響を受けやすい (are susceptible to vulnerabilities on one of the following ports)	構成済みのポートに関連付けられた潜在的な脆弱性を使用して、ネットワーク内のアセットをフィルタリングします。 指定したポート番号に基づいて、潜在的な脆弱性のあるアセットを識別するには、「ポート」パラメーターを構成します。
名前、ベンダー、バージョン、またはサービスに以下のいずれかのテキスト項目が含まれている、脆弱性の影響を受けやすい (are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries)	1 つ以上のテキスト項目に基づき、アセット名、ベンダー、バージョン、またはサービスと一致する、ネットワーク内の脆弱性を持つアセットをフィルタリングします。 「**テキスト項目 (text entries)**」パラメーターを構成して、このテストの対象とするアセット名、ベンダー、バージョン、またはサービスを指定します。
名前、ベンダー、バージョン、またはサービスに以下のいずれかの正規表現が含まれている、脆弱性の影響を受けやすい (are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions)	1 つ以上の正規表現に基づき、アセット名、ベンダー、バージョン、またはサービスと一致する、ネットワーク内の脆弱性を持つアセットをフィルタリングします。 「**正規表現**」パラメーターを構成して、このテストの対象とするアセット名、ベンダー、バージョン、またはサービスを指定します。
脆弱性の保存済み検索内に含まれる脆弱性の影響を受けやすい (are susceptible to vulnerabilities contained in vulnerability saved searches)	IBM Security QRadar Vulnerability Manager で作成された保存済み検索に関連付けられたリスクを検出します。

非推奨となった寄与テストの質問

テストは、別のテストに置き換えられると、ポリシー・モニターで非表示になります。

ポリシー・モニターで非表示になるテストは以下のとおりです。

- 以下のベンダーからの脆弱性の影響を受けやすいアセット (assets that are susceptible to vulnerabilities from the following vendors)
- 以下のサービスからの脆弱性の影響を受けやすいアセット (assets that are susceptible to vulnerabilities from the following services)

上記の寄与テストは、他のテストに置き換えられました。

可能な通信のテストの制限質問パラメーター

アセットの可能な通信のテストには、制限質問パラメーターがあります。

可能な通信のテストの制限質問パラメーターについて以下の表で説明します。

表 18. 可能な通信のテストの制限テスト

テスト名	説明
以下のプロトコルのみを含める (include only the following protocols)	構成されたプロトコルで通信したか通信しなかった可能性があるアセットを、この質問に追加された他のテストと共にフィルターに掛けます。
以下のインバウンド・ポートのみを含める (include only the following inbound ports)	構成されたポートで通信したか通信しなかった可能性があるアセットを、この質問に追加された他のテストと共にフィルターに掛けます。
以下のインバウンド・ポート以外のポートのみを含む (include only ports other than the following inbound ports)	構成されたポートで通信したか通信しなかった可能性がある、寄与テストの質問からのアセットを、この質問に追加された他のテストと共にフィルターに掛けます。
エクスプロイト可能な脆弱性の影響を受けやすい場合にのみ含める (include only if susceptible to vulnerabilities that are exploitable)	特定の脆弱性を探索する寄与テストの質問からのアセットをフィルターに掛け、結果をエクスプロイト可能なアセットに限定します。 この制限テストには構成可能なパラメーターは含まれませんが、寄与テスト「**以下の脆弱性のいずれかの影響を受けやすい (are susceptible to one of the following vulnerabilities)**」とともに使用されます。脆弱性パラメーターを含む、この要因となるルールは必須です。
以下のネットワークのみを含める (include only the following networks)	構成済みのネットワークのみを含むか、それらのネットワークを除外する寄与テストの質問からのアセットをフィルターに掛けます。
以下のアセット・ビルディング・ブロックのみを含める (include only the following asset building blocks)	構成済みのアセット・ビルディング・ブロックのみを含むか、それらのアセット・ビルディング・ブロックを除外する寄与テストの質問からのアセットをフィルターに掛けます。

表 18. 可能な通信のテストの制限テスト (続き)

テスト名	説明
以下のアセットの保存済み検索のみを含める (include only the following asset saved searches)	関連付けられたアセットの保存済み検索のみを含むか、それらの検索を除外する寄与テストの質問からのアセットをフィルターに掛けます。
以下のリファレンス・セットのみを含める (include only the following reference sets)	構成済みのもののみを含むか、それらを除外する寄与テストの質問からのアセットをフィルターに掛けます。
以下の IP アドレスのみを含める (include only the following IP addresses)	構成済みの IP アドレスのみを含むか、それらの IP アドレスを除外する寄与テストの質問からのアセットをフィルターに掛けます。
オペレーティング・システムの Microsoft Windows Service Pack が 0 未満の場合にのみ含める (include only if the Microsoft Windows service pack for operating systems is below 0)	アセットをフィルターに掛けて、オペレーティング・システムの Microsoft Windows Service Pack のレベルが、自社のポリシーで規定するレベル未満であるかどうかを判別します。
Microsoft Windows のセキュリティー設定が 0 未満の場合にのみ含める (include only if the Microsoft Windows security setting is less than 0)	アセットをフィルターに掛けて、Microsoft Windows のセキュリティー設定が、自社のポリシーで規定するレベル未満であるかどうかを判別します。
Microsoft Windows サービスが状況に等しい場合にのみ含める (include only if the Microsoft Windows service equals status)	アセットをフィルターに掛けて、Microsoft Windows サービスが不明、ブート、カーネル、自動、デマンド、または無効であるかどうかを判別します。
Microsoft Windows の設定が正規表現に一致する場合にのみ含める (include only if the Microsoft Windows setting equals regular expressions)	アセットをフィルターに掛けて、Microsoft Windows の設定が指定の正規表現に一致するかどうかを判別します。

デバイス/ルール・テストの質問

デバイス/ルール・テストの質問を使用して、定義済みのポリシーに違反していて、環境にリスクをもたらす可能性のあるデバイスのルールを識別します。

デバイス/ルール・テストの質問について、以下の表で説明します。

表 19. デバイス/ルール・テスト

テスト名	説明
以下のネットワークへの接続を許可する (allow connections to the following networks)	構成済みネットワークとの間におけるデバイス・ルールおよび接続をフィルタリングします。例えば、ネットワークへの通信を許可する際のテストを構成すると、テストで、構成済みネットワークへの接続を許可するすべてのルールと接続がフィルタリングされます。

表 19. デバイス/ルール・テスト (続き)

テスト名	説明
以下の IP アドレスへの接続を許可する (allow connections to the following IP addresses)	構成済み IP アドレスとの間におけるデバイス・ルールおよび接続をフィルタリングします。例えば、IP アドレスへの通信を許可する際のテストを構成すると、テストで、構成済み IP アドレスへの接続を許可するすべてのルールと接続がフィルタリングされます。
以下のアセット・ビルディング・ブロックへの接続を許可する (allow connections to the following asset building blocks)	構成済みアセット・ビルディング・ブロックとの間におけるデバイス・ルールおよび接続をフィルタリングします。
以下のリファレンス・セットへの接続を許可する (allow connections to the following reference sets)	構成済みリファレンス・セットとの間におけるデバイス・ルールおよび接続をフィルタリングします。
以下の宛先ポートおよびプロトコルを使用した接続を許可する (allow connections using the following destination ports and protocols)	構成済みのポートおよびプロトコルとの間におけるデバイス・ルールおよび接続をフィルタリングします。
以下のプロトコルを使用した接続を許可する (allow connections using the following protocols)	構成済みプロトコルとの間におけるデバイス・ルールおよび接続をフィルタリングします。
インターネットへの接続を許可する (allow connections to the Internet)	インターネットとの間におけるデバイス・ルールおよび接続をフィルタリングします。
以下のデバイスのいずれか (are one of the following devices)	すべてのネットワーク・デバイスをフィルタリングして、構成済みデバイスに絞ります。このテストでは、構成済みリストに含まれているデバイスであるかどうかに基づいてフィルタリングできます。
以下のリファレンス・セットのいずれか (are one of the following reference sets)	指定したリファレンス・セットに基づいてデバイス・ルールをフィルタリングします。
以下のネットワークのいずれか (are one of the following networks)	指定したネットワークに基づいてデバイス・ルールをフィルタリングします。
以下のアダプターのいずれかを使用する (are using one of the following adapters)	指定したアダプターに基づいてデバイス・ルールをフィルタリングします。

第 7 章 接続の調査

接続は、特定の時間間隔において検出された、特定の宛先ポートの 2 つの固有 IP アドレス間で行われた通信 (通信の拒否も含む) の記録です。

あるポートで同じ間隔で 2 つの IP アドレスが何度も通信した場合、記録される通信は 1 つだけですが、その接続での通信バイト数とフロー数は合計されます。間隔の終わりに、その間隔にわたる接続情報が集計されて、データベースに保管されます。

接続を使用して、ネットワーク・デバイスの接続をモニターおよび調査することも、拡張検索を行うこともできます。以下の操作を実行できます。

- 接続を検索する
- 接続のサブセットを検索する
- 検索結果をフォールス・ポジティブとしてマークし、作成されるオフェンスからフォールス・ポジティブ・イベントを除外するようチューニングする
- 各種オプションで接続情報をグループ化して表示する
- 接続を XML 形式または CSV 形式でエクスポートする
- 対話式グラフを使用して、ネットワーク内の接続を表示する

接続の表示

さまざまなオプションによってグループ化された接続情報を表示します。

このタスクについて

デフォルトでは、「接続」ウィンドウには、以下のグラフが表示されます。

- 「**時系列での一致したレコード**」グラフは、時間に基づいた接続の数を示す時系列情報を提供します。
- 「**接続グラフ**」は、取得された接続の視覚的な表現を提供します。

注: 保存済み検索がデフォルトである場合は、その保存済み検索の結果が表示されます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**接続**」をクリックします。
3. 「**開始時刻**」および「**終了時刻**」パラメーターを選択して時間フレームを選択するか、「**表示**」リストを使用します。

   表で、メニューの任意のセル (「**最後のパケットの時刻**」列のセルを除く) を右クリックして、さらにフィルタリングを適用するか、「**接続イベントの表示 (View Connection Events)**」を行います。

© Copyright IBM Corp. 2012, 2015

例

「接続」ウィンドウには、以下の情報が表示されます。

表 20. 「接続」ウィンドウ - デフォルト

パラメーター	説明
現在のフィルター (Current Filters)	このパラメーターはフィルターの適用後にのみ表示されます。 最上部に、検索結果に適用されるフィルターの詳細が表示されます。これらのフィルター値を消去するには、「**フィルターのクリア**」をクリックします。
表示 (View)	リストから、フィルタリングする時刻範囲を選択します。時刻範囲を調整するには、「**拡張 (Expand)**」オプションを使用します。
現在の統計	「現在の統計」には、以下のパラメーターが含まれます。 **合計結果数** - 検索条件に一致した結果の総数。 **検索されたデータ・ファイル** - 指定された期間内に検索されたデータ・ファイルの総数。 **検索された圧縮データ・ファイル** - 指定された期間内に検索された圧縮データ・ファイルの総数。 **索引ファイル数** - 指定された期間内に検索された索引ファイルの総数。 **期間** - 検索期間。 「**現在の統計**」はトラブルシューティングに役立ちます。問題のトラブルシューティングについて、お客様サポートに問い合わせたときに、現在の統計情報の提供を求められる場合があります。統計を表示または非表示にする場合は、「**現在の統計**」の横にある矢印をクリックしてください。.
グラフ (Charts)	時間間隔またはグループ・オプション (あるいはその両方) で一致したレコードを表すグラフを表示します。表示対象からグラフを除外する場合は、「**(グラフの非表示)**」をクリックします。 **注:** Firefox *Adblock Plus* が原因でグラフが Firefox に表示されない場合は、Adblock Plus を削除します。
最後のパケットの時刻 (Last Packet Time)	この接続でパケットが最後に処理された日時。

表 20. 「接続」ウィンドウ - デフォルト (続き)

パラメーター	説明
送信元タイプ	この接続の「**送信元タイプ**」。「**ホスト**」または「**リモート**」のいずれかです。
ソース	「**送信元**」のオプションは以下のとおりです。 **IP アドレス** - この接続の送信元の IP アドレス。「**送信元タイプ**」が「**ホスト**」である場合は、IP アドレスが表示されます。 **国 (Country)** - この接続の送信元の国 (および国旗)。国旗は、「送信元タイプ」が「リモート」である場合にのみ表示されます。
宛先タイプ	「**宛先タイプ**」のオプションは、「**ホスト**」または「**リモート**」のいずれかです。
宛先	「**宛先**」のオプションは以下のとおりです。 **IP アドレス** - 「宛先タイプ」が「ホスト」である場合は、IP アドレスが表示されます。 **国 (Country)** - この接続の宛先の国 (および国旗)。国旗は、「**宛先タイプ**」が「リモート」である場合にのみ表示されます。
プロトコル	この接続で使用されるプロトコル。
宛先ポート (Destination Port)	この接続の宛先ポート。
フロー・アプリケーション	接続を生成したフロー・アプリケーション。
フロー・ソース	この接続に関連付けられているフローのソース。このパラメーターは、受け入れられた接続にのみ適用されます。
フロー数	この接続に関連付けられているフローの総数。
フロー送信元バイト数	この接続に関連付けられているフロー送信元バイトの総数。
フロー宛先バイト数	この接続に関連付けられている宛先バイトの総数。
ログ・ソース	この接続に寄与するイベントのソース。
イベント数	接続で検出されたイベントの総数。
接続タイプ	「接続タイプ」のオプションは以下のとおりです。「**許可**」または「**拒否**」。

グラフを使用した接続データの表示

さまざまなグラフ・オプションを使用して接続データを表示することができます。デフォルトでは、時系列での一致したレコードおよび接続グラフを使用してデータを表示できます。

「時系列での一致したレコード」は、時刻に基づいて接続の数を示すオプションです。

接続グラフでは、取得した接続がビジュアル表示されます。接続グラフを使用して接続を詳細に調査する場合は、接続グラフの使用を参照してください。

グループ化された接続に使用可能なグラフ・オプションは表、棒、および円です。接続の検索について詳しくは、接続の検索を参照してください。

Mozilla Firefox Web ブラウザーで Adblock Plus ブラウザー拡張機能を使用すると、グラフが正常に表示されない場合があります。グラフを表示するには、Adblock Plus ブラウザー拡張機能を削除する必要があります。アドオンの削除について詳しくは、Web ブラウザーの資料を参照してください。

時系列グラフの使用

時系列グラフとは、時間の経過に応じて接続をグラフィカルに表現したものです。表示されるピークとくぼみは、接続アクティビティーの高低を示します。

始める前に

以前に検索をデフォルトとして保存していた場合、その保存済み検索の結果は「接続」ページに表示されます。その検索に「拡張ビュー定義」ボックスで選択された「グループ化の基準」オプションが含まれている場合、時系列グラフは使用できません。続行する前に検索条件をクリアする必要があります。

このタスクについて

時系列グラフは、データの短期および長期のトレンド分析に役立ちます。時系列グラフを使用すれば、さまざまな視点や角度から、接続に対するアクセス、ナビゲート、および調査を行うことができます。

次の表は、時系列グラフの表示に使用できる機能を示しています。

表 21. 時系列グラフの機能

操作	手順
接続をさらに詳細に表示する	時系列グラフでデータを拡大すると、さらに短い時間セグメントで接続を調査できます。時系列グラフは、次のいずれかのオプションを使用して拡大できます。 • Shift キーを押しながら、調査する時点をグラフ上でクリックします。 • Ctrl キーと Shift キーを押しながら、表示する時刻範囲をクリックしてマウス・ポインターでドラッグします。 • マウス・ポインターをグラフの上に移動してから、キーボードの上矢印を押します。 • マウス・ポインターをグラフの上に移動してから、マウス・ホイールを使用してズームインします (マウス・ホイールをロールアップ (画面上方送り) する)。 時系列グラフを拡大すると、グラフはさらに短い時間セグメントを表示するように更新されます。
さらに長い期間の接続を表示する	時系列グラフに追加の時刻範囲を含めると、さらに長い時間セグメントを調べることができます。または最大の時刻範囲に戻すことができます。次のいずれかのオプションを使用して、時刻範囲を表示できます。 • グラフの左上隅にある「最大」をクリックするか、または Home キーを押すと、最大の時刻範囲に戻ります。 • マウス・ポインターをグラフの上に移動してから、キーボードの下矢印を押します。 • マウス・ポインターをプロット・グラフの上に移動してから、マウス・ホイールを使用してズームアウトします (マウス・ホイールをロールダウン (画面下方送り) する)。
グラフをスキャンする	各データ・ポイントで情報を判別するためにグラフを表示するには、次のようにします。 • グラフをクリックおよびドラッグして、タイム・ラインをスキャンします。 • Page Up キーを押して、タイム・ラインを左側に 1 ページ分移動します。 • 左矢印キーを押して、タイム・ラインを左側に半ページ分移動します。 • Page Down キーを押して、タイム・ラインを右側に 1 ページ分移動します。 • 右矢印キーを押して、タイム・ラインを右側に半ページ分移動します。

手順

手順

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「**接続**」をクリックします。
3. グラフ・ペインで、「**構成**」アイコンをクリックします。
4. 「**グラフ・タイプ**」ドロップダウン・リストを使用して、「時系列」を選択します。
5. 対話式の時系列グラフを使用して、接続を調査するためにタイム・ライン全体をナビゲートできます。
6. グラフの情報を最新表示するには、「詳細の更新」をクリックします。

接続グラフを使用したネットワーク接続の表示

接続グラフでは、ネットワーク内の接続がビジュアル表示されます。

「接続」ウィンドウに表示されるグラフは対話式ではありません。グラフをクリックすると、「放射状データ・ビューアー」ウィンドウが表示されます。必要に応じて、「放射状データ・ビューアー」ウィンドウでグラフを操作できます。

デフォルトでは、グラフに以下のようにネットワーク接続が表示されます。

- 許可された接続のみを表示する。
- ローカル IP アドレスをすべて省略し、リーフ・ネットワークのみを表示する。
- 国別ノードをすべて「他国 (Remote Countries)」ノードにまとめる。
- リモート・ネットワーク・ノードをすべて「リモート・ネットワーク」という 1 つのノードにまとめる。
- グラフのプレビュー・サムネール表示に、メイン・グラフの一部を表示する。大規模なグラフの場合に便利です。

「放射状データ・ビューアー」には、以下のようなメニュー・オプションが用意されています。

表 22. 放射状データ・ビューアーのメニュー・オプション

メニュー・オプション	説明
接続タイプ	デフォルトでは、受け入れられた接続が放射状グラフに表示されます。拒否された接続を表示する場合は、「**接続タイプ**」ドロップダウン・リストから「拒否」を選択してください。
元に戻す (Undo)	最後に展開したノードを省略します。複数の展開を元に戻す場合は、展開ごとに「元に戻す (Undo)」ボタンをクリックします。

表 22. 放射状データ・ビューアーのメニュー・オプション (続き)

メニュー・オプション	説明
ダウンロード	現在のトポロジーを JPEG 画像ファイルまたは Visio 図面ファイル (VDX) として保存するには、「**ダウンロード**」をクリックします。 現在のトポロジーを Visio 図面ファイル (VDX) としてダウンロードして保存する場合に必要な最小ソフトウェア・バージョンは Microsoft Visio Standard 2010 です。

接続を表示するための追加機能を以下の表に示します。

表 23. 放射状データ・ビューアーの機能

操作	手順
ズームインまたはズームアウトする	グラフの右上にあるスライダーを使用してスケールを変更します。
グラフのノードを配置し直して追加の詳細を表示する	ノードを任意の位置にドラッグして、グラフのノードを配置し直します。
ネットワーク・ノードを展開する	ノードをダブルクリックすると、そのノードのアセットが展開されて表示されます。ノードを展開すると、そのノードの通信先アセットが表示されます。デフォルトでは、この展開操作はネットワークの最初の 100 件のアセットに制限されています。
接続に関する詳細を表示する	接続線にマウス・ポインターを合わせると、追加の詳細が表示されます。 ネットワーク・ノードとリモート・ネットワークまたは他国との接続である場合は、右クリックすると、以下の「**送信元**」メニューおよび「**フローの表示 (View Flows)**」メニューが表示されます。 2 つの IP アドレスの間の接続である場合は、接続線をクリックすると、送信元、宛先、およびポートの情報が表示されます。
接続に関連するデータの量を判断する	グラフにおける線の太さは、その接続に関連するデータの量を示します。線が太いほどデータ量が多いことを示します。この情報は、通信に使用されたバイト数から導き出されます。
接続パスを強調表示する	接続線にマウス・ポインターを合わせます。その接続が許可されている場合は、パスが緑で強調表示されます。その接続が拒否されている場合は、パスが赤で強調表示されます。

表 23. 放射状データ・ビューアーの機能 (続き)

操作	手順
特定のノードの接続パスを判別する	ノードにマウス・ポインターを合わせます。そのノードが許可されている場合は、そのノードへのパスとノード自体が緑で強調表示されます。そのノードが拒否されている場合は、そのノードへのパスとノード自体が赤で強調表示されます。
グラフ・ビューを変更する	プレビュー・サムネールを使用して、サムネールを、表示したいグラフの部分に移動します。

円グラフ、棒グラフ、および表グラフの使用

円グラフ、棒グラフ、または表グラフを使用して、接続データを表示できます。

このタスクについて

円グラフ、棒グラフ、および表グラフのオプションは、検索に「拡張ビュー定義」オプションで選択された「グループ化の基準」が含まれている場合にのみ表示されます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**接続**」をクリックします。

   注: デフォルトの保存済み検索結果が表示されます。
3. 検索を実行します。
4. グラフ・ペインで、「**構成**」アイコンをクリックします。
5. 以下のパラメーターを構成します。

オプション	説明
グラフの値	「**グラフの値**」リストを使用して、グラフで表すオブジェクト・タイプを選択します。このオプションには、使用している検索パラメーターに含まれている、正規化されたパラメーターおよびカスタム・フローのパラメーターがすべて含まれます。
グラフ・タイプ	「**グラフ・タイプ**」リストを使用して、表示するグラフ・タイプを選択します。以下のオプションがあります。 • **表** - データを表形式で表示します。 • **棒** - データを棒グラフで表示します。 • **円** - データを円グラフで表示します。

6. 「**保存**」をクリックします。

検索条件が自動的に詳細を表示するようになっていない限り、データが自動的に最新表示されることはありません。

7. データを最新表示するには、「**詳細の更新**」をクリックします。

接続の検索

特定の条件を使用して接続を検索し、検索条件に一致する接続を結果リストに表示することができます。新しい検索を作成することも、以前に保存された一連の検索条件をロードすることもできます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**接続**」をクリックします。

   該当する場合、デフォルトの保存済み検索結果が表示されます。
3. 「**検索**」リストを使用して、「**新規検索**」を選択します。
4. 以前に保存した検索をロードする場合は、次のいずれかのオプションを使用します。
   a. 「**グループ**」リストから、保存済み検索を関連付けるグループを選択します。
   b. 「**使用可能な保存済み検索**」リストから、ロードする保存済み検索を選択します。
   c. 「**保存済み検索の入力またはリストから選択**」フィールドに、ロードする検索の名前を入力します。「使用可能な保存済み検索」リストから、ロードする保存済み検索を選択します。
   d. 「**ロード**」をクリックします。
   e. 「**検索の編集**」ペインで、この検索に必要なオプションを選択します。

オプション	説明
クイック検索に含める	この検索を「クイック検索」項目に含めます。
ダッシュボードに含める	保存済み検索からのデータをダッシュボードに含めます。このパラメーターは、検索がグループ化されている場合にのみ選択可能です。
デフォルトとして設定	この検索をデフォルトの検索として設定します。
全員と共有	これらの検索要件を他のすべての IBM Security QRadar Risk Manager ユーザーと共有します。

5. 「時刻範囲」ペインで、この検索用にキャプチャーする時刻範囲のオプションを選択します。

オプション	説明
最新	リストを使用して、フィルタリングする時刻範囲を指定します。

オプション	説明
特定の間隔	カレンダーを使用して、フィルタリングする日時範囲を指定します。

6. 検索の構成が終了し、結果を表示する場合は、「検索」をクリックします。
7. 「検索パラメーター」ペインで、以下のように具体的な検索条件を定義します。
   a. 最初のリストを使用して、検索する属性を選択します。例えば、接続タイプ、送信元ネットワーク、または方向などです。
   b. 2 番目のリストを使用して、検索に使用する修飾子を選択します。表示される修飾子のリストは、最初のリストで選択した属性によって異なります。
   c. テキスト・フィールドに、検索に関連する具体的な情報を入力します。
   d. 「**フィルターの追加**」をクリックします。
   e. 検索条件に追加するフィルターごとに、a から e までのステップを繰り返します。
   f. 検索の構成が終了し、結果を表示する場合は、「**検索**」をクリックします。そうしない場合は、次のステップに進みます。
8. 検索の完了時に検索結果を自動的に保存する場合は、「検索の完了時に結果を保存」チェック・ボックスを選択して、名前を指定します。
9. 検索の構成が終了し、結果を表示する場合は、「**検索**」をクリックします。そうしない場合は、次のステップに進みます。
10. 「列定義」ペインを使用して、結果の表示に使用する列および列のレイアウトを定義します。
    a. 「**表示**」リストを使用して、この検索に関連付けるビューを選択します。
    b. 「**拡張ビュー定義**」の横にある矢印をクリックして、拡張検索パラメーターを表示します。パラメーターを非表示にするには、矢印を再度クリックします。
11. 「**検索**」をクリックします。

検索条件の保存

検索条件を指定して検索を作成し、その検索を将来の使用のために保存することができます。

このタスクについて

検索結果に表示される列をカスタマイズできます。以下のオプションは「列定義」セクションで選択でき、「拡張ビュー定義」オプションと呼ばれています。

表 24. 「拡張ビュー定義」オプション

パラメーター	説明
列を入力するか、リストから選択してください	「使用可能な列」リストの列をフィルタリングします。 見つける列の名前を入力するか、またはキーワードを入力してそのキーワードが含まれる列名のリストを表示します。 例えば、「**送信元**」を入力すると、列名に「送信元」が含まれている列のリストが表示されます。
使用可能な列	選択したビューに関連付けられている使用可能な列をリストします。この保存済み検索で現在使用されている列が、「**列**」リスト内で強調表示されます。
列ボタンの追加と削除 (上部セット) (Add and remove column buttons (top set))	上部セットのボタンを使用して、「**グループ化の基準**」リストをカスタマイズできます。 • 「**列の追加**」 - 「**使用可能な列**」リストから 1 つ以上の列を選択し、「**列の追加**」ボタンをクリックします。 • 「**列の削除**」 - 「**グループ化の基準**」リストから 1 つ以上の列を選択し、「**列の削除**」ボタンをクリックします。
列ボタンの追加と削除 (下部セット) (Add and remove column buttons (bottom set))	下部セットのボタンを使用して、「**列**」リストをカスタマイズできます。 • 「**列の追加**」 - 「**使用可能な列**」リストから 1 つ以上の列を選択し、「**列の追加**」ボタンをクリックします。 • 「**列の削除**」 - 「**列**」リストから 1 つ以上の列を選択し、「**列の削除**」ボタンをクリックします。
グループ化の基準	保存済み検索の結果をグループ化する列を指定します。次のオプションを使用して、「**グループ化の基準**」リストをさらにカスタマイズできます。 • 「**上に移動**」 - 列を選択し、「**上に移動**」アイコンを使用してその列を優先順位リスト内で上に移動します。 • 「**下に移動**」 - 列を選択し、「**下に移動**」アイコンを使用してその列を優先順位リスト内で下に移動します。 優先順位リストは、結果をグループ化する順序を指定します。検索結果は、「**グループ化の基準**」リストの 1 列目でグループ化された後、リストの次の列でグループ化されます。

表 24. 「拡張ビュー定義」オプション (続き)

パラメーター	説明
列	検索に対して選択される列を指定します。列は保存済み検索からロードされます。「**列**」リストは、列を「**使用可能な列**」リストから選択することでカスタマイズできます。次のオプションを使用して、「**列**」リストをさらにカスタマイズできます。 • 「**上に移動**」 - 列を選択し、「上に移動」ボタンを使用してその列を優先順位リスト内で上に移動します。 • 「**下に移動**」 - 列を選択し、「下に移動」ボタンを使用してその列を優先順位リスト内で下に移動します。 列のタイプが数値または時刻であるときに、「**グループ化の基準**」リストに項目がある場合は、列のグループ化方法を選択できるように、列にドロップダウン・リストが組み込まれます。
順序	最初のリストを使用して、検索結果のソート基準となる列を指定します。次に、2 番目のリストを使用して、検索結果を表示する順序 (「**降順**」または「**昇順**」) を指定します。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**接続**」をクリックします。
3. 検索を実行します。
4. 「**条件の保存**」をクリックします。
5. 次の各パラメーターの値を構成します。

オプション	説明
検索名	この検索条件に割り当てる名前を入力します。
グループへの検索の割り当て	この保存済み検索に割り当てるグループ。グループを選択しない場合は、この保存済み検索がデフォルトで「その他」グループに割り当てられます。
タイム・スパン・オプション	次のオプションのいずれかを選択してください。 • 「最新」 - ドロップダウン・リストを使用して、フィルタリングする時刻範囲を指定します。 • 「特定の間隔」 - カレンダーを使用して、フィルタリングする日時範囲を指定します。

オプション	説明
クイック検索に含める	この検索を「クイック検索」項目 (「**検索**」ドロップダウン・リストにあります) に含める場合は、このチェック・ボックスを選択します。
ダッシュボードに含める	保存済み検索からのデータをダッシュボードに含める場合は、このチェック・ボックスを選択します。 このパラメーターは、検索がグループ化されている場合にのみ表示されます。
デフォルトとして設定	この検索をデフォルトの検索として設定する場合は、このチェック・ボックスを選択します。
全員と共有	これらの検索要件を他のすべての IBM Security QRadar Risk Manager ユーザーと共有する場合は、このチェック・ボックスを選択します。

6. 「**OK**」をクリックします。

サブ検索の実行

検索を実行するたびに、条件と一致する接続を見つけるためにデータベース全体が照会されます。このプロセスは、データベースのサイズによっては、かなり時間がかかる場合があります。

このタスクについて

サブ検索は、一連の完了した検索結果内で検索を実行できます。データベースを再度検索しなくても、検索結果を絞り込むことができます。サブ検索は、グループ化された検索または進行中の検索には使用できません。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**接続**」をクリックします。
3. 検索を実行します。 検索結果が表示されます。サブ検索の実行時に、追加の検索は、直前の検索のデータ・セットを使用します。
4. フィルターを追加するには、以下のステップを実行します。
   a. 「**フィルターの追加**」をクリックします。
   b. 最初のリストを使用して、検索する属性を選択します。
   c. 2 番目のリストを使用して、検索に使用する修飾子を選択します。表示される修飾子のリストは、最初のリストで選択した属性によって異なります。
   d. テキスト・フィールドに、検索に関連する具体的な情報を入力します。
   e. 「**フィルターの追加**」をクリックします。

注: 検索が進行中のままである場合、部分的な結果が表示されます。「元のフィルター」ペインは、元の検索でベースになったフィルターを示します。「現在のフィルター」ペインは、サブ検索に適用されたフィルターを示します。

ヒント: サブ検索フィルターは、元の検索を再開しなくてもクリアできます。クリアするフィルターの隣にある「フィルターのクリア」リンクをクリックします。「元のフィルター」ペインからフィルターをクリアする場合は、元の検索が再実行されます。

5. サブ検索を保存するには、「**条件の保存**」をクリックします。

タスクの結果

元の検索を削除する場合、保存済みのサブ検索にアクセスできます。フィルターを追加すると、サブ検索機能による検索は以前に検索されたデータ・セットにはもはや基づかなくなるため、サブ検索はデータベース全体を検索します。

検索結果の管理

他のインターフェースにナビゲートするときに、複数の接続検索を実行できます。

このタスクについて

検索の完了時に E メール通知が送信されるように検索機能を構成できます。検索の進行中にはいつでも、進行中の検索の部分的な結果を表示できます。

検索結果ツールバーには、次のオプションがあります。

パラメーター	説明
新規検索	新規検索を作成する場合は、「**新規検索 (New Search)**」をクリックします。このボタンをクリックすると、検索ウィンドウが表示されます。
結果の保存	検索結果を保存するには、「**結果の保存**」をクリックします。 このオプションは、「検索結果の管理」リストで行を選択している場合にのみ有効です。
キャンセル	進行中の検索または開始するためにキューに入っている検索をキャンセルするには、「**キャンセル**」をクリックします。
削除	検索結果を削除する場合は、「**削除**」をクリックします。
通知	通知を受け取るようにする検索を選択し、次に「**通知**」をクリックして、検索の完了時の E メール通知を有効にします。

パラメーター	説明
表示	ドロップダウン・リストで、検索結果ウィンドウにリストする検索結果を指定します。オプションは次のとおりです。 • 保存済み検索結果 (Saved Search Results) • すべての検索結果 (All Search Results) • キャンセルされた検索/エラーが発生した検索 (Canceled/Erroneous Searches) • 進行中の検索 (Searches in Progress)

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**接続**」をクリックします。
3. メニューから、「**検索**」 > 「**検索結果の管理**」を選択します。

検索結果の保存

検索結果を保存することができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**接続**」をクリックします。
3. 接続検索またはサブ検索を実行します。
4. 「検索結果」ウィンドウから、「**検索**」 > 「**検索結果の管理**」を選択して、検索結果を選択します。
5. 「**結果の保存 (Save Results)**」をクリックします。
6. 検索結果の名前を入力します。
7. 「**OK**」をクリックします。

検索のキャンセル

1 つ以上の検索をキャンセルすることができます。

このタスクについて

キャンセルしたときに検索が進行中であった場合は、検索のキャンセルまでに蓄積された結果が保持されます。

手順

1. 「検索結果の管理」ウィンドウで、キューに入っている検索または進行中の検索結果から、キャンセルするものを選択します。キャンセル対象として複数の検索を選択することができます。
2. 「**検索のキャンセル (Cancel Search)**」をクリックします。
3. 「**はい**」をクリックします。

検索結果の削除

検索を削除することができます。

手順

1. 「検索結果の管理」ウィンドウで、削除する検索結果を選択します。
2. 「**削除**」をクリックします。
3. 「**はい**」をクリックします。

接続のエクスポート

接続は XML (Extensible Markup Language) 形式 または CSV (Comma Separated Values) 形式でエクスポートできます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**接続**」をクリックします。
3. 接続を XML 形式でエクスポートするには、「**アクション**」 > 「**XML にエクスポート**」を選択します。
4. 接続を CSV 形式でエクスポートするには、「**アクション**」>「**CSV にエクスポート**」を選択します。
5. アクティビティーを再開するには、「**完了時に通知 (Notify When Done)**」をクリックします。

第 8 章 ログ・ソース・マッピング

ファイアウォール・ルールのトリガー頻度をモニターしたり、トポロジー・イベントの検索を使用可能にしたりする際に、IBM Security QRadar Risk Manager は QRadar のログ・ソースを識別します。

ファイアウォール・ルールを理解することで、ファイアウォールの効率性を維持し、セキュリティー・リスクを防ぐことができます。

QRadar Risk Manager では、1 つのログ・ソースに最大 255 のデバイスをマップできますが、デバイスに複数のログ・ソースがある場合があります。

ログ・ソース・マッピングの表示オプション

ネットワーク・デバイスを QRadar のログ・ソースとして構成した場合、「構成モニター (Configuration Monitor)」ページの「**ログ・ソース**」列には、以下のいずれかの項目が表示されます。

- **自動マップ済み (Auto-Mapped)** - QRadar Risk Manager がログ・ソースを識別して自動的にデバイスにマップする場合。
- **ユーザー名** - 管理者がログ・ソースを手動で追加または変更した場合。
- **空白** - QRadar Risk Manager がデバイスのログ・ソースを識別できない場合、「**ログ・ソース**」列には値が表示されません。手動でログ・ソース・マッピングを作成できます。

ログ・ソースの構成について詳しくは、*IBM Security QRadar Log Sources User Guide* を参照してください。

ログ・ソース・マッピングの作成または編集

IBM Security QRadar Risk Manager が QRadar 内のログ・ソースを識別できない場合、ログ・ソース・マッピングを構成できます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・ペインで、「**構成モニター (Configuration Monitor)**」をクリックします。
3. ログ・ソース・マッピングのないデバイスをクリックします。
4. ツールバーで、「**アクション**」 > 「**ログ・ソース・マッピング (Log Source Mapping)**」 > 「**ログ・ソース・マッピングの作成/編集 (Create/Edit Log Source Mapping)**」をクリックします。
5. 「**ログ・ソース・グループ**」リストで、グループを選択します。
6. 「**ログ・ソース**」リストでログ・ソースを選択し、(**>**) をクリックします。
7. 「**OK**」をクリックします。

© Copyright IBM Corp. 2012, 2015

第 9 章 ネットワーク・デバイス構成の調査

IBM Security QRadar Risk Manager では、ネットワーク・デバイスの効率を管理したり、ファイアウォール・ルールを調査したり、無効なファイアウォール・ルールにより発生したセキュリティー・リスクを特定したりできます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・ペインで、「**構成モニター (Configuration Monitor)**」をクリックします。
3. ネットワーク・デバイスを検索するには、IP アドレスまたはホスト名を「**IP アドレスまたはホスト名の入力 (Input IP Address or Host Name)**」フィールドに入力します。
4. 調査するデバイスをダブルクリックします。

   ルールの「**イベント数**」列には、ファイアウォール・ルールのトリガー頻度が表示されます。ゼロのイベント数ルールは、次のいずれかの理由で表示されます。

   - ルールがトリガーされず、セキュリティー・リスクの原因となっている可能性があります。ファイアウォール・デバイスを調査して、トリガーされないルールをすべて削除することができます。
   - QRadar のログ・ソース・マッピングが構成されていません。
5. ルールを検索するには、「**ルール**」ツールバーで、「**検索**」 > 「**新規検索**」をクリックします。

   アイコンが「**状況**」列に表示される場合は、マウス・ポインターを状況アイコン上に移動すると、詳細情報を表示できます。
6. デバイス・インターフェースを調査するには、ツールバーで「**インターフェース**」をクリックします。
7. アクセス制御リスト (ACL) デバイス・ルールを調査するには、ツールバーで「**ACL**」をクリックします。

   各アクセス制御リストは、ネットワーク上のデバイスの通信に使用されるインターフェースを定義します。 ACL の条件が満たされると、ACL に関連付けられているルールがトリガーされます。各ルールは、デバイス間の通信を許可または拒否するかをテストされます。
8. ネットワーク・アドレス変換 (NAT) デバイス・ルールを調査するには、ツールバーで「**NAT**」をクリックします。

   「**フェーズ (Phase)**」列は、例えばルーティングの前または後など、NAT ルールをトリガーするタイミングを示します。
9. 履歴を調査したり、デバイス構成を比較したりするには、ツールバーで「**履歴**」をクリックします。

© Copyright IBM Corp. 2012, 2015

デバイス・ルールは、正規化された比較ビューまたはロー・デバイス構成で表示できます。正規化されたデバイス構成は、デバイス間の追加、削除、または変更されたルールを表示する、グラフィカルな比較です。ロー・デバイス構成は、デバイス・ファイルの XML ビューまたはプレーン・テキスト・ビューです。

デバイス・ルールの検索

IBM Security QRadar Risk Manager では、トポロジー内のデバイスで変更されたルールを検索できます。また、デバイス構成バックアップ間で行うルールの変更もディスカバーできます。

ルール検索で返される結果は、デバイスの構成ソース管理バックアップに基づくものになります。ルール検索で確実に最新情報が提供されるようにするために、ファイアウォール・ポリシーの更新ページでデバイス・バックアップをスケジュールできます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・ペインで、「**構成モニター (Configuration Monitor)**」をクリックします。
3. 「構成モニター (Configuration Monitor)」ページでデバイスをダブルクリックします。
4. 「ルール」ペインのツールバーで、「**検索**」 > 「**新規検索**」をクリックします。
5. 「**検索条件**」領域で、時刻範囲をクリックします。
6. デバイス・ルールを検索するには、次のオプションのいずれかを選択します。
   - 「**シャドーイング済み**」、「**削除済み**」、または「**その他**」の各ルールを検索するには、状況オプションをクリックします。

     デフォルトではすべての状況オプションが有効になります。シャドー・ルールのみを検索するには、「**削除済み**」オプションと「**その他**」オプションをクリアします。
   - アクセス制御リスト (ACL) を検索するには、「**リスト**」フィールドに入力します。
   - ルール項目の順序番号で検索するには、「**項目**」フィールドに数値を入力します。
   - 送信元または宛先を検索するには、IP アドレス、CIDR アドレス、ホスト名、またはオブジェクト・グループ参照を入力します。
   - ポートまたはオブジェクト・グループ参照を検索するには、「**サービス**」フィールドに入力します。

     サービスには、ポート範囲 (例えば、100-200)、またはポート式 (例えば、80(TCP)) を含めることができます。ポートを否定する場合、ポート情報には感嘆符も含まれ、また括弧で囲むことができます (例えば、!(100-200) または !80(TCP))。
   - IPS デバイスによって定義されている脆弱性ルール情報を検索するには、「**シグネチャー**」フィールドに入力します。

- アダプターでアプリケーションを検索するには、「**アプリケーションの選択 (Select Applications)**」をクリックして、アダプター名またはアプリケーション名を入力します。

7. 「**検索**」をクリックします。

ネットワーク・デバイスの構成の比較

IBM Security QRadar Risk Manager では、単一のデバイスの複数のバックアップを比較するか、2 つのネットワーク・デバイス・バックアップを比較することによって、デバイス構成を相互に比較することができます。

共通の構成タイプには以下の項目を含めることができます。

- **標準エレメント文書 (Standard Element Document)** - 標準エレメント文書 (SED) ファイルは、ネットワーク・デバイスに関する情報を含む XML データ・ファイルです。個々の SED (標準エレメント文書) ファイルは未加工の XML 形式で表示されます。SED (標準エレメント文書) ファイルを別の SED (標準エレメント文書) ファイルと比較する場合は、表示が正規化され、ルールの違いが表示されます。
- **構成** - 構成ファイルは、デバイスのメーカーに応じて、特定のネットワーク・デバイスに提供されます。構成ファイルを表示するにはダブルクリックします。

アダプターがデバイスについて収集する情報によっては、他の複数の構成タイプが表示される場合があります。これらのファイルをダブルクリックすると、プレーン・テキストで表示されます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**構成モニター (Configuration Monitor)**」をクリックします。
3. デバイスをダブルクリックすると、詳細な構成情報が表示されます。
4. 「**履歴**」をクリックすると、そのデバイスの履歴が表示されます。
5. 単一のデバイスの 2 つの構成を比較するには、以下のようにします。
   a. プライマリー構成を選択します。
   b. Ctrl キーを押しながら、比較対象の別の構成を選択します。
   c. 「履歴」ペインで、「**選択した項目を比較 (Compare Selected)**」をクリックします。

      比較ファイルが標準エレメント文書 (SED) である場合は、「正規化されたデバイス構成の比較 (Normalized Device Configuration Comparison)」ウィンドウに、バックアップ間のルールの違いが表示されます。

      正規化された構成を比較するときには、テキストの色によって以下のデバイス更新が示されます。

      - 輪郭が緑の点線の場合は、デバイスに追加されたルールまたは構成を示します。
      - 輪郭が赤い破線の場合は、デバイスから削除されたルールまたは構成を示します。

- 輪郭が黄色の実線の場合は、デバイスで変更されたルールまたは構成を示します。

d. 未加工の構成の違いを表示するには、「**未加工での比較を表示 (View Raw Comparison)**」をクリックします。

構成ファイルまたは別のバックアップ・タイプを比較する場合は、未加工での比較が表示されます。

6. 異なるデバイスの 2 つの構成を比較するには、以下のようにします。
   a. デバイスからのプライマリー構成を選択します。
   b. 「**比較対象のマークを付ける (Mark for Comparison)**」をクリックします。
   c. ナビゲーション・メニューから「**すべてのデバイス (All Devices)**」を選択し、デバイス・リストに戻ります。
   d. 比較するデバイスをダブルクリックし、「**履歴**」をクリックします。
   e. マークを付けた構成と比較する構成を選択します。
   f. 「**マークしたものと比較 (Compare with Marked)**」をクリックします。
   g. 未加工の構成の違いを表示するには、「**未加工での比較を表示 (View Raw Comparison)**」をクリックします。

第 10 章 ユーザーまたはグループによるデバイス・ルールのフィルター操作

QRadar Risk Manager では、ユーザーまたはグループによるデバイス・ルールの表示およびフィルター操作をすることができます。

このタスクについて

ユーザーまたはグループでルールの対話を検索し、標準的なユーザーまたはグループがネットワーク内でどのように対話するかを把握します。ネットワークでのユーザーのルールの対話を把握することは、誤った動作の検出や、ネットワークでの効率的なルール・ポリシーの策定に役立ちます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**構成モニター (Configuration Monitor)**」をクリックします。
3. 「**デバイス・リスト (Device List)**」テーブルで、ご使用のデバイスのテーブル行をダブルクリックします。

   ルール・テーブルの「**ユーザー/グループ (User(s)/Group(s))**」列で、ユーザーとグループを表示できます。
4. 「ルール」ペインで、「**検索**」 > 「**新規検索**」をクリックします。
5. ユーザー名またはグループ名を「**ユーザーまたはグループ (User or Group)**」フィールドに入力します。
6. 「**検索**」をクリックします。

   検索ストリングがユーザー名またはグループ名の一部と一致する場合、そのユーザー名またはグループ名にリンクされているルールが表示されます。

   このルール情報を使用して、ユーザー・ルールの対話に対してベンチマークまたはプロファイルを設定します。これはネットワークでのルール・ポリシーを最適化するために使用できます。

© Copyright IBM Corp. 2012, 2015

第 11 章 IBM Security QRadar Risk Manager レポートの管理

ネットワーク・デバイスに関するレポートを作成、編集、配布、および管理することができます。PCI コンプライアンスなどのさまざまな規制基準を満たすために、ファイアウォール・ルール、およびデバイス間の接続に関する詳細レポートが必要になることがよくあります。

以下のレポート・オプションは、QRadar Risk Manager に固有です。

表 25. QRadar Risk Manager のレポート・オプション

レポート・オプション	説明
接続	指定した時間フレームで発生した、ネットワーク・デバイスの接続図。
デバイス・ルール	指定した時間フレームでネットワーク・デバイスに構成されたルール。このレポート・オプションを使用して、1 つ以上のネットワーク・デバイスについて、以下のルール・タイプを表示できます。 • 最も使用頻度の高い容認ルール • 最も使用頻度の高い否認ルール • 最も使用頻度の低い容認ルール • 最も使用頻度の低い否認ルール • シャドーイング済みルール • 使用されていないオブジェクト・ルール
デバイス未使用オブジェクト	デバイスで使用されていないすべてのオブジェクト参照グループの名前、構成日時、および定義を示す表を生成します。オブジェクト参照グループとは、IP アドレス、CIDR アドレス、ホスト名、ポート、およびその他のデバイス・パラメーターのコレクションを表すために使用される総称です。これらはグループ化され、デバイスのルールに割り当てられます。

レポートの手動生成

レポートは、手動で開始できます。複数のレポートを手動で開始すると、それらのレポートはキューに追加され、各レポートに、キュー内でのその位置を示すラベルが付けられます。

© Copyright IBM Corp. 2012, 2015

このタスクについて

レポートを手動で生成しても、既存のレポート・スケジュールはリセットされません。例えば、最もアクティブなファイアウォール拒否についての週次レポートを生成する場合、このレポートは手動で生成し、週次レポートは引き続き、初めに構成したスケジュールに従って生成します。

レポートが生成されると、「**次の実行時刻**」列に、次の 3 つのメッセージのいずれかが表示されます。

- 「**生成中 (Generating)**」 - レポートは生成中です。
- 「**待機中 (キューで待機) (Queued (position in the queue))**」 - レポートは生成を待機中です。このメッセージには、キュー内のレポートの位置が示されます。例えば、「1 of 3」などです。
- 「**(x 時間 x 分 y 秒) ((x hour(s) x min(s) y sec(s)))**」 - レポートは実行をスケジュールされています。このメッセージは、レポートが次にいつ実行されるかを示すカウントダウン・タイマーです。

手順

1. 「**レポート**」タブをクリックします。
2. 生成するレポートを選択します。
3. 「**レポートの実行**」をクリックします。
4. オプション。「**最新表示**」をクリックします。「**次の実行時刻**」列の情報を含め、ビューが最新表示されます。

次のタスク

レポートを生成した後、「**生成済みレポート**」列からレポートを表示できます。

レポート・ウィザードの使用

レポート・ウィザードを使用して、新規のレポートを作成することができます。レポート・ウィザードでは、レポートの設計、スケジューリング、および生成の手順が段階的に示されます。

このウィザードでは、以下の主要な要素を使用してレポートの作成を支援します。

- **レイアウト** - 各コンテナーの位置とサイズ
- **コンテナー** - レポートのコンテンツのプレースホルダーまたは位置
- **コンテンツ** - IBM Security QRadar Risk Manager がコンテナーのグラフに含めるレポート・データを定義します。

レポートのレイアウトを選択する際は、作成するレポートのタイプに配慮してください。例えば、多数のオブジェクトを表示するグラフ・コンテンツの場合は、小さなグラフ・コンテナーを選択しないでください。各グラフには、凡例と、コンテンツの派生元になったネットワークのリストが含まれます。それらのデータを格納できる十分な大きさのコンテナーを選択してください。

週に 1 回または月に 1 回生成されるレポートの場合、スケジュールされた時間が経過してからでないと、生成されるレポートは結果を返しません。スケジュールさ

れたレポートの場合は、スケジュールされた時間が経過するまでレポートが作成されません。例えば、週に 1 回の検索では、データが作成されるまでに 7 日間を要します。この検索では、7 日後に結果が返されます。

レポートの作成

特定の間隔のレポートを作成し、グラフ・タイプを選択することができます。

このタスクについて

レポートは複数のデータ・エレメントから構成することができ、ネットワークおよびセキュリティーのデータを、表、折れ線グラフ、円グラフ、棒グラフなどのさまざまなスタイルで表現できます。

レポートの配布オプションとして「レポート・コンソール」または E メールを指定できます。以下の表に、これらの配布オプションのパラメーターを示します。

表 26. 生成されたレポートの配布オプション

オプション	**説明**
レポート・コンソール	生成されたレポートを「**レポート**」タブに送信する場合は、このチェック・ボックスを選択します。これはデフォルトの配布チャネルです。
このレポートにより生成された出力を表示可能にするユーザーを選択してください。	このオプションは、「**レポート・コンソール**」チェック・ボックスを選択した場合にのみ表示されます。 ユーザーのリストから、生成されたレポートを表示する権限を付与する IBM Security QRadar Risk Manager ユーザーを選択します。 生成されたレポートを他のユーザーと共有するには、適切なネットワーク権限が必要です。権限の詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

表 26. 生成されたレポートの配布オプション (続き)

オプション	説明
すべてのユーザーを選択 (Select all users)	このオプションは、「**レポート・コンソール**」チェック・ボックスを選択した場合にのみ表示されます。 生成されたレポートを表示する権限をすべての QRadar Risk Manager ユーザーに付与する場合は、このチェック・ボックスを選択します。 生成されたレポートを他のユーザーと共有するには、適切なネットワーク権限が必要です。権限の詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
E メール	生成されたレポートを E メールで配布する場合は、このチェック・ボックスを選択します。
レポートの宛先 E メール・アドレスの入力 (複数可) (Enter the report destination email address(es))	このオプションは、「**E メール**」チェック・ボックスを選択した場合にのみ表示されます。 生成されたレポートの各受信者の E メール・アドレスを入力します。E メール・アドレス間はコンマで区切ってください。このパラメーターの最大長は 255 文字です。 E メールの受信者は、このメールを no_reply_reports@qradar から受け取ります。
レポートを添付ファイルとして含める (HTML 以外のみ)	このオプションは、「**E メール**」チェック・ボックスを選択した場合にのみ表示されます。 生成されたレポートを添付ファイルとして送信する場合は、このチェック・ボックスを選択します。
レポート・コンソールへのリンクを含める	このオプションは、「**E メール**」チェック・ボックスを選択した場合にのみ表示されます。 E メールにレポート・コンソールへのリンクを含める場合は、このチェック・ボックスを選択します。

手順

1. 「**レポート**」タブをクリックします。
2. 「**アクション**」リストから「**作成 (Create)**」を選択します。

3. 「**次へ**」をクリックしてレポート・ウィザードの次のページに移動します。
4. レポート・スケジュールの頻度を選択します。
5. 「このレポートの手動生成を許可しますか」ペインで、このレポートの手動生成を有効にするは「**はい**」を、無効にするには「**いいえ**」を選択します。このオプションは、手動で生成されたレポートでは使用できません。
6. 「**次へ**」をクリックします。
7. レポートのレイアウトを選択し、「**次へ**」をクリックします。
8. レポート・タイトルを入力します。タイトルの最大長は 100 文字です。特殊文字は使用しないでください。
9. ロゴを選択します。QRadar のロゴがデフォルトのロゴです。レポートのブランド設定について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
10. 「**グラフ・タイプ**」リストから、QRadar Risk Manager 固有のレポートのいずれかを選択します。
11. グラフ用にレポート・データを構成します。
12. 「**コンテナー詳細の保存**」をクリックします。
13. 「**次へ**」をクリックします。
14. レポート・フォーマットを選択します。複数のオプションを選択できます。

    注: 「デバイス・ルール」および「使用されていないオブジェクト・ルール (Unused Object Rules)」レポートでは、PDF、HTML、および RTF のレポート・フォーマットのみがサポートされます。
15. 「**次へ**」をクリックします。
16. レポートで使用する配布チャネルを選択します。
17. 「**次へ**」をクリックします。
18. このレポートの説明を入力します。この説明は、「レポートのサマリー」ページおよび生成されたレポートの配布 E メールに表示されます。
19. このレポートを割り当てるグループを選択します。グループについて詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」で、『レポートの管理 (Managing Reports)』を参照してください。
20. オプション。ウィザードのセットアップが完了したときにこのレポートを実行するには「はい」を選択します。「**次へ**」をクリックしてレポートのサマリーを表示します。サマリー・レポートで使用可能なタブを選択して、レポートの選択をプレビューできます。
21. 「**終了**」をクリックします。

タスクの結果

レポートは即時に生成されます。ウィザードの最後のページで「**今すぐこのレポートを実行しますか?**」チェック・ボックスをクリアした場合は、レポートは保存され、スケジュールに従って生成されます。

レポート・タイトルは、生成されるレポートのデフォルトのタイトルです。レポートを再構成して新しいレポート・タイトルを入力すると、レポートが新しい名前を持つ新規のレポートとして保存され、元のレポートはそのまま保持されます。

レポートの編集

レポートを編集して、レポート・スケジュール、レイアウト、構成、タイトル、フォーマット、および配信方式を調整できます。既存のレポートを編集するか、デフォルトのレポートを編集することができます。

手順

1. 「**レポート**」タブをクリックします。
2. 編集するレポートを選択します。
3. 「**アクション**」リストから、「**編集**」を選択します。
4. 新規レポート・スケジュールの頻度を選択します。
5. 「このレポートの手動生成を許可しますか」ペインで、以下のオプションのいずれかを選択します。
   - **はい** - このレポートの手動生成を有効にします。
   - **いいえ** - このレポートの手動生成を無効にします。
6. 「**次へ**」をクリックしてレポート・ウィザードの次のページに移動します。
7. レポートのレイアウトを構成します。
   a. 「**方向**」リストから、ページの向きを選択します。
   b. IBM Security QRadar Risk Manager レポートのレイアウト・オプションを選択します。
   c. 「**次へ**」をクリックします。
8. 次の各パラメーターの値を指定します。
   - 「**レポート・タイトル**」 - レポート・タイトルを入力します。タイトルの最大長は 100 文字です。特殊文字は使用しないでください。
   - 「**ロゴ**」 - リストからロゴを選択します。QRadar のロゴがデフォルトのロゴです。レポートのブランド設定について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
9. レポート・データのコンテナーを構成します。
   a. 「**定義**」をクリックします。
   b. グラフ用にレポート・データを構成します。
   c. 「**コンテナー詳細の保存**」をクリックします。
   d. 必要に応じて、これらのステップを繰り返して追加コンテナーを編集します。
   e. 「**次へ**」をクリックしてレポート・ウィザードの次のページに移動します。
10. 「**次へ**」をクリックしてレポート・ウィザードの次のステップに移動します。
11. レポート・フォーマットのチェック・ボックスを選択します。複数のオプションを選択できます。

    注: QRadar Risk Manager 固有のレポート (「デバイス・ルール」レポートや「デバイス未使用オブジェクト」レポートなど) では PDF、HTML、および RTF フォーマットのみがサポートされます。
12. 「**次へ**」をクリックしてレポート・ウィザードの次のページに移動します。
13. レポートの配布チャネルを選択します。

14. 「**次へ**」をクリックしてレポート・ウィザードの最後のステップに移動します。
15. このレポートの説明を入力します。この説明は、「レポートのサマリー」ページおよび生成されたレポートの配布 E メールに表示されます。
16. このレポートを割り当てるグループを選択します。グループについて詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」で、『レポートの管理 (Managing Reports)』を参照してください。
17. オプション。ウィザードのセットアップが完了したときにこのレポートを実行するには「はい」を選択します。
18. 「**次へ**」をクリックしてレポートのサマリーを表示します。「レポートのサマリー」ページが表示され、レポートの詳細が示されます。サマリー・レポートで使用可能なタブを選択して、レポートの選択をプレビューできます。
19. 「**終了**」をクリックします。

レポートの複製

任意のレポートを複製できます。

手順

1. 「**レポート**」タブをクリックします。
2. コピーするレポートを選択します。
3. 「**アクション**」リストから「**コピー (Duplicate)**」を選択します。
4. レポートに対し、スペースを含まない新しい名前を入力します。

レポートの共有

レポートを他のユーザーと共有することができます。レポートを共有する場合は、他のユーザーが編集やスケジュールするために、選択したレポートのコピーを提供します。

始める前に

レポートを共有するには管理特権が必要になります。また、新規ユーザーがレポートを表示し、レポートにアクセスするためには、管理ユーザーが、この新規ユーザーと必要なすべてのレポートを共有する必要があります。

このタスクについて

ユーザーが共有レポートを更新しても、元のバージョンのレポートには影響しません。

手順

1. 「**レポート**」タブをクリックします。
2. 共有するレポートを選択します。
3. 「**アクション**」リストで、「**共有 (Share)**」をクリックします。
4. ユーザーのリストから、このレポートを共有するユーザーを選択します。

適切なアクセス権限を持つユーザーを選択できない場合は、メッセージが表示されます。

5. 「**共有**」をクリックします。

レポートについて詳しくは、『*IBM Security QRadar SIEM ユーザーズ・ガイド*』を参照してください。

グラフの構成

グラフのタイプによって、グラフに構成されて表示されるデータが決まります。デバイスで収集したデータに固有の複数のグラフを IBM Security QRadar Risk Manager で作成できます。

以下のグラフ・タイプは、QRadar Risk Manager に固有です。

- 接続
- デバイス・ルール
- デバイス未使用オブジェクト

接続グラフ

接続グラフを使用して、ネットワーク接続の情報を表示できます。これらのグラフは、「リスク」タブの保存済み接続検索のデータに基づいて作成できます。

生成されるレポートで表示するデータをカスタマイズすることができます。構成可能な期間にわたってデータを作図するようにグラフを構成することができます。この機能は、接続の傾向を検出するために役立ちます。

以下の表に、接続グラフ・コンテナーの構成情報を記載します。

表 27. 接続グラフのパラメーター

パラメーター	説明
コンテナー詳細 - 接続	
グラフ・タイトル (Chart Title)	グラフのタイトルを最大 100 文字で入力します。
グラフ・サブタイトル	自動的に作成されたサブタイトルを変更するには、このチェック・ボックスをクリアします。タイトルは最大 100 文字で入力します。

表 27. 接続グラフのパラメーター (続き)

パラメーター	説明
グラフ・タイプ (Graph Type)	リストから、生成されるレポートに表示するグラフのタイプを選択します。以下のオプションがあります。 • **棒** - データを棒グラフで表示します。これはデフォルトのグラフ・タイプです。このタイプのグラフの場合、保存された検索はグループ化された検索である必要があります。 • **折れ線** - データを折れ線グラフで表示します。 • **円** - データを円グラフで表示します。このタイプのグラフの場合、保存された検索はグループ化された検索である必要があります。 • **積み重ね棒** - データを積み重ね棒グラフで表示します。 • **積み重ね線** - データを積み重ね折れ線グラフで表示します。 • **表** - データを表形式で表示します。「**表**」オプションは、全ページ幅コンテナーでのみ使用することができます。
グラフ	生成されるレポートに表示する接続の数をリストから選択します。
手動スケジュール	「手動スケジュール (Manual Scheduling)」ペインは、レポート・ウィザードで「**手動 (Manually)**」スケジュール・オプションを選択した場合にのみ表示されます。 手動スケジュールを作成するには、以下の手順を実行します。 1. 「**開始日 (From)**」リスト・ボックスでレポートの開始日を入力するか、「**カレンダー (Calender)**」アイコンを使用して日付を選択します。デフォルトは現在日付です。 2. リスト・ボックスで、レポートの開始時刻を選択します。時刻は、30 分単位で指定できます。デフォルトは 1:00 a.m. です。 3. 「**終了日 (To)**」リストでレポートの終了日を入力するか、「**カレンダー (Calender)**」アイコンを使用して日付を選択します。デフォルトは現在日付です。 4. リストで、レポートの終了時刻を選択します。時刻は、30 分単位で指定できます。デフォルトは 1:00 a.m. です。

表 27. 接続グラフのパラメーター (続き)

パラメーター	説明
毎時スケジュール	「毎時スケジュール (Hourly Scheduling)」ペインは、レポート・ウィザードで「**毎時 (Hourly)**」スケジュール・オプションを選択した場合にのみ表示されます。 毎時スケジュールでは、直近 1 時間のすべてのデータが自動的にグラフ化されます。
日次スケジュール	「日次スケジュール」ペインは、レポート・ウィザードで「**毎日**」スケジュール・オプションを選択した場合にのみ表示されます。 次のオプションのいずれかを選択してください。 • **直近 1 日 (24 時間) の全データ** • **次からの直近 1 日のデータ** - 生成されるレポートに適用する期間をリストから選択します。時刻は、30 分単位で指定できます。デフォルトは 1:00 a.m. です。
週次スケジュール	「週次スケジュール」ペインは、レポート・ウィザードで「**毎週**」スケジュール・オプションを選択した場合にのみ表示されます。 次のオプションのいずれかを選択してください。 • **直近 1 週間の全データ** • **次からの直近 1 週間のデータ** - 生成されるレポートに適用する期間をリストから選択します。デフォルトは日曜日です。
月次スケジュール	「月次スケジュール」ペインは、レポート・ウィザードで「**毎月**」スケジュール・オプションを選択した場合にのみ表示されます。 次のオプションのいずれかを選択してください。 • **直近 1 カ月の全データ (All data from previous month)** • **次からの直近 1 カ月のデータ** - 生成されるレポートに適用する期間をリストから選択します。デフォルトは 1 日から 31 日までです。
グラフ・コンテンツ	
グループ	リストから、保存済み検索グループを選択して「**使用可能な保存済み検索**」リスト内のそのグループに属している保存済み検索を表示します。

表 27. 接続グラフのパラメーター (続き)

パラメーター	説明
保存済み検索の入力またはリストから選択	「**使用可能な保存済み検索**」リストの詳細な指定を行うには、目的の検索名を「**保存済み検索の入力またはリストから選択**」フィールドに入力します。キーワードを入力して、そのキーワードを含む検索のリストを表示させることもできます。例えば DMZ と入力すると、検索名に「DMZ」が含まれるすべての検索のリストが表示されます。
使用可能な保存済み検索	使用可能な保存済み検索のリストが表示されます。デフォルトでは、使用可能なすべての保存済み検索が表示されます。ただし、「**グループ**」リストからグループを選択するか、「**保存済み検索を入力するか、リストから選択してください**」フィールドに既知の保存済み検索の名前を入力することにより、リストをフィルタリングできます。
新規接続検索の作成	新規検索を作成する場合は、「**新規接続検索の作成**」をクリックします。

デバイス・ルール・グラフ

デバイス・ルール・グラフを使用して、ファイアウォール・ルールと、ネットワーク内でトリガーされたファイアウォール・ルールのイベント数を確認できます。

デバイス・ルール・レポートでは、以下のファイアウォール・ルールに関するレポートを作成できます。

- 最もアクティブな容認デバイス・ルール
- 最もアクティブな否認デバイス・ルール
- 最もアクティブでない容認デバイス・ルール
- 最もアクティブでない否認デバイス・ルール
- 使用されていないデバイス・ルール
- シャドーイング済みデバイス・ルール

生成したレポートで、単一のデバイス、特定のアダプター、あるいは複数のデバイスで受け入れられたルール、拒否されたルール、使用されていないルール、トリガーされていないルールを把握できます。レポートを使用することで、IBM Security QRadar Risk Manager がデバイス・ルールの状況に関するレポート作成を自動化し、IBM Security QRadar SIEM コンソールにレポートを表示できるようになります。

この機能は、ネットワーク・デバイスでのルールの使用状況を識別するのに役立ちます。

デバイス・ルール・グラフ・コンテナーを作成するには、以下のパラメーターの値を構成します。

表 28. デバイス・ルール・グラフのパラメーター

パラメーター	説明
コンテナー詳細 - デバイス・ルール	
上位のルールに限定 (Limit Rules to Top)	生成後のレポートに表示するルールの数をリストから選択します。 例えば、レポートを上位 10 件のルールに限定して、デバイス全体で最も使用頻度の高い容認ルールのレポートを作成すると、レポートは 10 件の結果を返します。結果には、QRadar Risk Manager に表示されるデバイス全体のイベント数に基づき、最も使用頻度の高い 10 件のルールがリストされます。
タイプ (Type)	レポートに表示するデバイス・ルールのタイプを選択します。以下のオプションがあります。 • **最も使用頻度の高い容認ルール** - 単一のデバイスまたはデバイスのグループでのイベント数による、最も使用頻度の高い容認ルールを表示します。このレポートは、レポートに指定した時間フレームで容認イベント数が最も多いルールを降順でリストします。 • **最も使用頻度の高い否認ルール** - 単一のデバイスまたはデバイスのグループでのイベント数による、最も使用頻度の高い否認ルールを表示します。このレポートは、レポートに指定した時間フレームで否認イベント数が最も多いルールを降順でリストします。 • **使用されていないルール** - 単一のデバイスまたはデバイスのグループで使用されていないルールをすべて表示します。使用されていないルールは、レポートに指定した時間フレームでのイベント数がゼロになります。 • **最も使用頻度の低い容認ルール** - 単一のデバイスまたはデバイスのグループで最も使用頻度の低い容認ルールを表示します。このレポートは、レポートに指定した時間フレームで容認イベント数が最も少ないルールを昇順でリストします。 • **最も使用頻度の低い否認ルール** - 単一のデバイスまたはデバイスのグループで最も使用頻度の低い否認ルールを表示します。このレポートは、レポートに指定した時間フレームで否認イベント数が最も少ないルールを昇順でリストします。 • **シャドーイング済みルール** - 後続するルールによってブロックされるため、トリガーできない、単一デバイスのルールをすべて表示します。結果には、シャドーを生成しているルールと、デバイス上の後続するルールによってシャドーイングされるためにデバイスでトリガーできないルールのテーブルが表示されます。 **注:** シャドーイング済みルールのレポートは、単一のデバイスに対してのみ実行できます。このルールは、レポートに指定した時間フレームでのイベント数がゼロになり、「状況」列のアイコンで識別されます。

表 28. デバイス・ルール・グラフのパラメーター (続き)

パラメーター	説明
日付/時刻範囲	レポートの時間フレームを選択します。以下のオプションがあります。 • **現在の構成 (Current Configuration)** - デバイス・ルール・レポートの結果は、現在のデバイス構成内に存在するルールに基づきます。このレポートは、既存のデバイス構成のルールとイベント数を表示します。 デバイスの現在の構成は、構成ソース管理でネットワーク・デバイスが最後にバックアップされた時点に基づきます。 • **間隔** - デバイス・ルール・レポートの結果は、この間隔の時間フレームに存在していたルールに基づきます。このレポートは、過去 1 時間から 30 日間までの指定した間隔におけるルールとイベント数を表示します。 • **特定の範囲 (Specific Range)** - デバイス・ルール・レポートの結果は、開始時刻から終了時刻までの時刻範囲内に存在していたルールに基づきます。このレポートは、指定した時間フレームでのルールとイベント数を表示します。
タイム・ゾーン	レポートの基礎として使用するタイム・ゾーンを選択します。デフォルトのタイム・ゾーンは、QRadar SIEM コンソール の構成に基づきます。 レポートの「タイム・ゾーン」パラメーターを構成する際は、レポートされるデータに関連付けられたデバイスの場所を考慮してください。レポートが複数のタイム・ゾーンにわたってデータを使用する場合、レポートに使用されるデータは、構成されたタイム・ゾーンの特定の時刻範囲に基づきます。 例えば、QRadar SIEM コンソール が東部標準時 (EST) で構成されていて、午後 1 時から午後 3 時の間に日次レポートをスケジュールし、タイム・ゾーンを中央標準時 (CST) として設定すると、レポートの結果には、EST の午後 2 時から 4 時までの情報が含まれることになります。

表 28. デバイス・ルール・グラフのパラメーター (続き)

パラメーター	説明
ターゲット・データの選択	「ターゲット・データの選択」は、「日付/時刻範囲」をフィルターに掛けて特定の値に絞り込む際に使用します。「ターゲット・データの選択」オプションを使用すると、選択した時間と日付のデータのみを含めるオプションを指定して、カスタム定義された期間にわたるデバイス・ルールを表示するレポートを作成できます。 例えば、10 月 1 日から 10 月 31 日までの期間にレポートを実行するようにスケジュールし、営業時間内 (月曜日から金曜日の午前 8 時から午後 9 時までなど) で最もアクティブなルール、最もアクティブでないルール、または使用されていないルールとそのイベント数を表示することができます。 **注:** フィルターの詳細は、レポート・ウィザードで「**ターゲット・データの選択**」チェック・ボックスを選択した場合にのみ表示されます。
形式	デバイス・ルール・レポートの形式を選択します。以下のオプションがあります。 • **指定したすべてのデバイスに対する 1 つの集約レポート (One aggregate report for specified devices)** - このレポート形式では、複数のデバイスのレポート・データが集約されます。 例えば、上位 10 件の最も使用頻度の高い否認ルールを表示するレポートを作成する場合、集約レポートには、レポート対象として選択したデバイス全体で最も使用頻度の高い上位 10 件の否認ルールが表示されます。このレポートは、合計 10 件の結果を返します。 • **デバイスごとに 1 つのレポート (One report per device)** - このレポート形式では、デバイスごとにレポート・データが表示されます。 例えば、上位 10 件の最も使用頻度の高い否認ルールを表示するレポートを作成する場合、集約レポートには、レポート対象として選択したデバイスごとに、最も使用頻度の高い上位 10 件の否認ルールが表示されます。このレポートは、レポート対象として選択したデバイスごとに、上位 10 件の結果を返します。5 つのデバイスを選択すると、レポートは 50 件の結果を返します。 **注:** シャドーイング済みルールのレポートで表示できるのは、デバイスごとに 1 つのレポートのみです。

表 28. デバイス・ルール・グラフのパラメーター (続き)

パラメーター	説明
デバイス	レポートに含めるデバイスを選択します。以下のオプションがあります。 • **すべてのデバイス** - QRadar Risk Manager のすべてのデバイスをレポートに含めるようにする場合、このオプションを選択します。 • **アダプター** - リストから、レポートに含めるアダプター・タイプを選択します。リストからレポートに対して選択できるアダプター・タイプは 1 つのみです。 • **特定のデバイス (Specific Devices)** - 特定のデバイスのみをレポートに含めるようにする場合、このオプションを選択します。「デバイスの選択 (Device Selection)」ウィンドウで、デバイスを選択してレポートに追加できます。 個々のデバイスをレポートに追加するには、以下のようにします。 1. 「**参照**」をクリックして「デバイスの選択 (Device Selection)」ウィンドウを表示します。 2. 任意のデバイスを選択し、「**選択項目の追加**」をクリックします。 すべてのデバイスをレポートに追加するには、以下のようにします。 1. 「**参照**」をクリックして「デバイスの選択 (Device Selection)」ウィンドウを表示します。 2. 「**すべて追加 (Add All)**」をクリックします。 レポートに含めるデバイスを検索するには、以下のようにします。 1. 「**参照**」をクリックして「デバイスの選択 (Device Selection)」ウィンドウを表示します。 2. 「**検索**」をクリックします。 3. 検索オプションを選択し、取得した構成、IP アドレスまたは CIDR アドレス、ホスト名、タイプ、アダプター、ベンダー、またはモデルで、全デバイスのリストをフィルタリングします。 4. 「**検索**」をクリックします。 5. 任意のデバイスを選択し、「**選択項目の追加**」をクリックします。

デバイス未使用オブジェクト・グラフ

デバイス未使用オブジェクト・レポートには、ネットワーク・デバイスで使用されていないオブジェクト参照グループが表示されます。

このレポートには、ネットワーク・デバイスで使用されていないオブジェクト参照 (IP アドレス、CIDR アドレス範囲、またはホスト名の集合) が表示されます。

デバイス未使用オブジェクト・コンテナーの構成時は、以下のパラメーターの値を構成します。

表 29. デバイス未使用オブジェクト・レポートのパラメーター

パラメーター	説明
コンテナー詳細 - デバイス未使用オブジェクト	
上位のオブジェクトに限定 (Limit Objects to Top)	生成後のレポートに表示するルールの数をリストから選択します。
デバイス	レポートに含めるデバイスを選択します。以下のオプションがあります。 • **すべてのデバイス** - IBM Security QRadar Risk Manager のすべてのデバイスをレポートに含めるようにする場合、このオプションを選択します。 • **アダプター** - リストから、レポートに含めるアダプター・タイプを選択します。リストからレポートに対して選択できるアダプター・タイプは 1 つのみです。 • **特定のデバイス (Specific Devices)** - 特定のデバイスのみをレポートに含めるようにする場合、このオプションを選択します。「デバイスの選択 (Device Selection)」ウィンドウで、デバイスを選択してレポートに追加できます。 個々のデバイスをレポートに追加するには、以下のようにします。 1. 「**参照**」をクリックして「デバイスの選択 (Device Selection)」ウィンドウを表示します。 2. 任意のデバイスを選択し、「**選択項目の追加**」をクリックします。 すべてのデバイスをレポートに追加するには、以下のようにします。 1. 「**参照**」をクリックして「デバイスの選択 (Device Selection)」ウィンドウを表示します。 2. 「**すべて追加 (Add All)**」をクリックします。 レポートに含めるデバイスを検索するには、以下のようにします。 1. 「**参照**」をクリックして「デバイスの選択 (Device Selection)」ウィンドウを表示します。 2. 「**検索**」をクリックします。 3. 検索オプションを選択し、取得した構成、IP アドレスまたは CIDR アドレス、ホスト名、タイプ、アダプター、ベンダー、またはモデルで、全デバイスのリストをフィルタリングします。 4. 「**検索**」をクリックします。 5. 任意のデバイスを選択し、「**選択項目の追加**」をクリックします。

第 12 章 ポリシー管理

アセット、ポリシー、ポリシー検査について、ポリシー・コンプライアンスとポリシー・リスクの変更に関する詳細を表示するには、IBM Security QRadar Risk Manager のポリシー管理ページを使用します。

QRadar Risk Manager のポリシー管理ページには、最後に実行されたポリシーのデータが表示されます。このデータは、アセット、ポリシー、またはポリシー検査でフィルタリングすることができます。

ポリシー管理のユース・ケース

コンプライアンスに準拠していないアセットとポリシーに関する詳細情報を確認するには、ポリシー管理ページの「**リスク**」ダッシュボードの項目を使用します。

- 「**アセット別**」ページには、アセットが不合格になったポリシーの情報とリンクが表示されます。
- 「**ポリシー別 (By Policy)**」ページには、合格したアセットと不合格になったアセットの数とパーセンテージに関する情報が表示されます。また、該当する場合は、ポリシーが使用するポリシー検査のリンクも表示されます。
- 「**ポリシー検査別 (By Policy Check)**」ページには、個別のポリシー検査に合格したアセットと不合格になったアセットの数とパーセンテージに関する情報が表示されます。

リスクの増加を示しているポリシーとポリシー検査を調べるには、ポリシー管理ページの「**リスクの変化**」ダッシュボードの項目を使用します。「**リスクの変化**」ダッシュボードの項目には、「**ポリシー別 (By Policy)**」ページと「**ポリシー検査別 (By Policy Checks)**」ページへのリンクが表示されます。

「**リスク**」ダッシュボードと「**リスクの変化**」ダッシュボードの項目について詳しくは、「*IBM Security QRadar SIEM ユーザーズ・ガイド*」を参照してください。

© Copyright IBM Corp. 2012, 2015

第 13 章 IBM Security QRadar Risk Manager でのシミュレーションの使用

ネットワークでのエクスプロイト・シミュレーションを定義し、スケジュールして実行するには、シミュレーションを使用します。シミュレーションの作成、表示、編集、複製、および削除が可能です。

組み合わせと構成が可能な一連のルールに基づいてシミュレーションを作成できます。シミュレーションは、定期的に実行するようにスケジュールすることも、手動で実行することもできます。シミュレーションが完了したら、シミュレーションの結果を確認し、ネットワーク・ポリシーに基づいて、結果のうち、許容できるものやリスクの低いものを承認できます。結果の確認時に、結果のうちの許容できるアクションやトラフィックを承認できます。シミュレーションをチューニングしてから、結果をモニターするようにそのシミュレーションを構成できます。

シミュレーションをモニターするときには、承認されない結果が返された場合にシステムにどのように応答させるかを定義できます。システム応答としては E メール、イベントの作成、または syslog への応答の送信が可能です。

シミュレーションは、現在のトポロジーまたはトポロジー・モデルからモデル化することができます。

「シミュレーション」ページには、シミュレーションおよびシミュレーション結果に関する情報がまとめられます。

シミュレーションが完了しなければシミュレーション結果は表示されません。シミュレーションが完了すると、シミュレーションの日付および対応する結果が「**結果**」列にリストされます。

シミュレーション

ユーザーによって作成されたシミュレーションおよびシミュレーション結果は、「シミュレーション」ページから表示できます。

「シミュレーション」ウィンドウには以下の情報が表示されます。

表 30. シミュレーション定義のパラメーター

パラメーター	説明
シミュレーション名 (Simulation Name)	シミュレーションの名前。シミュレーションの作成者によって定義されたものです。
モデル	モデルのタイプ。シミュレーションは、現在のトポロジーまたはトポロジー・モデルからモデル化することができます。オプションは次のとおりです。 • 現在のトポロジー (Current Topology) • トポロジー・モデルの名前。

© Copyright IBM Corp. 2012, 2015

表 30. シミュレーション定義のパラメーター (続き)

パラメーター	説明
グループ	このシミュレーションが関連付けられているグループ。
作成者	このシミュレーションを作成したユーザー。
作成日	このシミュレーションが作成された日時。
最終変更日時	最後にこのシミュレーションが変更された日時。
スケジュール	シミュレーションをスケジュール実行する頻度。以下のオプションがあります。 • **手動** - シミュレーションは、手動で実行したときに実行されます。 • **1 回 (Once)** - シミュレーションをスケジュール実行する日時を指定します。 • **毎日** - シミュレーションをスケジュール実行する時刻を指定します。 • **毎週** - シミュレーションをスケジュール実行する曜日と時刻を指定します。 • **毎月** - シミュレーションをスケジュール実行する日付と時刻を指定します。
最終実行 (Last Run)	最後にこのシミュレーションが実行された日時。
次の実行 (Next Run)	次のシミュレーションが実行される日時。
結果	シミュレーションの実行が完了している場合は、シミュレーションの結果を含む日付のリストを含むリストがこのパラメーターに表示されます。まだシミュレーションが実行されていない場合、「結果」列には「結果なし (No Results)」と表示されます。

シミュレーションの作成

組み合わせと構成が可能な一連のルールに基づいてシミュレーションを作成できます。

このタスクについて

シミュレーション・テスト用に構成可能なパラメーターには下線が付けられています。以下の表で、構成できるシミュレーション・テストについて説明します。

表 31. シミュレーション・テスト

テスト名	説明	パラメーター
以下の IP アドレスのいずれかを対象とした攻撃 (Attack targets one of the following IP addresses)	特定の IP アドレスまたは CIDR 範囲に対する攻撃をシミュレートします。	このシミュレーションを適用する IP アドレスまたは CIDR 範囲を指定するための IP アドレス・パラメーターを構成します。

表 31. シミュレーション・テスト (続き)

テスト名	説明	パラメーター
以下のネットワークのいずれかを対象とした攻撃 (Attack targets one of the following networks)	1 つ以上の定義済みネットワーク・ロケーションのメンバーであるネットワークを対象とする攻撃をシミュレートします。	このシミュレーションを適用するネットワークを指定するネットワーク・パラメーターを構成します。
以下のアセット・ビルディング・ブロックのいずれかを対象とした攻撃 (Attack targets one of the following asset building blocks)	1 つ以上の定義済みアセット・ビルディング・ブロックを対象とする攻撃をシミュレートします。	このシミュレーションを適用するアセット・ビルディング・ブロックを指定するアセット・ビルディング・ブロック・パラメーターを構成します。
以下のリファレンス・セットのいずれかを対象とした攻撃 (Attack targets one of the following reference sets)	1 つ以上の定義済みリファレンス・セットを対象とする攻撃をシミュレートします。	このシミュレーションを適用するリファレンス・セットを指定するリファレンス・セット・パラメーターを構成します。
プロトコルを使用する以下のいずれかのポートの脆弱性を対象とした攻撃 (Attack targets a vulnerability on one of the following ports using protocols)	1 つ以上の定義済みポートの脆弱性を対象とした攻撃をシミュレートします。	以下のパラメーターを構成します。 • 開いているポート - このシミュレーションの対象とするポートを指定します。 • プロトコル - このシミュレーションの対象とするプロトコルを指定します。
以下の脆弱性のいずれかの影響を受けやすいアセットを対象とした攻撃 (Attack targets assets susceptible to one of the following vulnerabilities)	1 つ以上の定義済み脆弱性の影響を受けやすいアセットを対象とした攻撃をシミュレートします。	「**脆弱性**」パラメーターを構成して、このテストを適用する脆弱性を指定します。 OSVDB ID、Bugtraq ID、CVE ID、またはタイトルで脆弱性を検索できます。
以下のいずれかの分類の脆弱性の影響を受けやすいアセットを対象とした攻撃 (Attack targets assets susceptible to vulnerabilities with one of the following classifications)	1 つ以上の定義済み分類の脆弱性の影響を受けやすいアセットを対象とする攻撃をシミュレートできるようにします。	「**分類**」パラメーターを構成して脆弱性分類を指定します。例えば、脆弱性分類として、入力操作 (Input Manipulation) やサービス妨害 (Denial of Service) などがあります。

表 31. シミュレーション・テスト (続き)

テスト名	説明	パラメーター
CVSS スコアが 5 より大きい脆弱性の影響を受けやすいアセットを対象とした攻撃 (Attack targets assets susceptible to vulnerabilities with CVSS score greater than 5)	共通脆弱性評価システム (CVSS) の値は、脆弱性の重大度を評価するための業界標準です。このシミュレーションでは、構成された CVSS 値を含むネットワーク内のアセットをフィルタリングします。 CVSS スコアが 5 よりも大きい脆弱性の影響を受けやすいアセットを対象とした攻撃をシミュレートすることができます。	以下のパラメーターを構成します。 • **より大** - 共通脆弱性評価システム (CVSS) スコアが、構成された値に対して、「より大」、「以上」、「より小」、「以下」、「次に等しい」、「次と等しくない」のいずれであるかを指定します。デフォルトは「より大」です。 • **5** - このテストの対象とする CVSS スコアを指定します。デフォルトは 5 です。
この日付よりも後に公開された脆弱性の影響を受けやすいアセットを対象とした攻撃 (Attack targets assets susceptible to vulnerabilities disclosed after this date)	構成された日付よりも前、後、またはその日にディスカバーされた脆弱性の影響を受けやすいアセットを対象とした攻撃をシミュレートすることができます。	以下のパラメーターを構成します。 • **より前 | より後 | 該当日** - シミュレーションで対象とする資産に対する脆弱性を、構成された日よりも前、後、またはその日のいずれに公開されたものにするかを指定します。デフォルトは「より前」です。 • **この日付 (this date)** - このシミュレーションの対象とする日付を指定します。
名前、ベンダー、バージョン、またはサービスに以下のいずれかのテキスト項目が含まれている、脆弱性の影響を受けやすいアセットを対象とした攻撃 (Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries)	1 つ以上のテキスト項目に基づいてアセット名、ベンダー、バージョン、またはサービスに一致する、脆弱性の影響を受けやすいアセットを対象とした攻撃をシミュレートできるようにします。	**「テキスト項目 (text entries)」**パラメーターを構成して、このシミュレーションの対象とするアセット名、ベンダー、バージョン、またはサービスを指定します。

表 31. シミュレーション・テスト (続き)

テスト名	説明	パラメーター
名前、ベンダー、バージョン、またはサービスが以下のいずれかの正規表現を含む、脆弱性の影響を受けやすいアセットを対象とした攻撃 (Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions)	1 つ以上の正規表現に基づいてアセット名、ベンダー、バージョン、またはサービスに一致する、脆弱性の影響を受けやすいアセットを対象とした攻撃をシミュレートできるようにします。	「**正規表現 (regular expressions)**」パラメーターを構成して、このシミュレーションの対象とするアセット名、ベンダー、バージョン、またはサービスを指定します。

以下の提供テストは非推奨となっており、ポリシー・モニターでは非表示になっています。

- **以下のいずれかのオペレーティング・システムの脆弱性を対象とした攻撃 (attack targets a vulnerability on one of the following operating systems)**
- **以下のいずれかのベンダーからの脆弱性の影響を受けやすいアセットを対象とした攻撃 (attack targets assets susceptible to vulnerabilities from one of the following vendors)**
- **以下のいずれかの製品の脆弱性の影響を受けやすいアセットを対象とした攻撃 (attack targets assets susceptible to vulnerabilities from one of the following products)**

非推奨の提供テストは他のテストにより置き換えられています。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 「**アクション**」メニューから、「**新規**」を選択します。
4. 「**このシミュレーションの名前の指定 (What do you want to name this simulation)**」パラメーターにシミュレーションの名前を入力します。
5. 「**ベースとするモデルの選択 (Which model do you want to base this on)**」ドロップダウン・リストで、返すデータのタイプを選択します。既存のすべてのトポロジー・モデルがリストされます。「**現在のトポロジー (Current Topology)**」を選択した場合、シミュレーションでは現在のトポロジー・モデルを使用します。
6. 次のオプションのいずれかを選択してください。

オプション	説明
「**接続データを使用する (Use Connection Data)**」を選択する	シミュレーションは接続データおよびトポロジー・データに基づきます。

オプション	説明
「接続データを使用する (Use Connection Data)」をクリアする	シミュレーションはトポロジー・データのみに基づきます。 トポロジー・モデルにデータが含まれていない場合、**「接続データを使用する」**チェック・ボックスをクリアすると、シミュレーションから結果が返されません。

7. **「重要度係数 (Importance Factor)」**リストから、このシミュレーションに関連付ける重要度のレベルを選択します。

   「重要度係数 (Importance Factor)」はリスク・スコアを計算するために使用されます。範囲は 1 (低重要度) から 10 (高重要度) までです。デフォルトは 5 です。

8. **「シミュレーションの開始場所 (Where do you want the simulation to begin)」**リストから、シミュレーションのオリジンを選択します。

   選択した値によりシミュレーションの開始点が決定されます。例えば、特定のネットワークが発信元である攻撃などです。選択したシミュレーション・パラメーターが**「次のシミュレーションを生成 (Generate a simulation where)」**ウィンドウに表示されます。

9. シミュレーション攻撃のターゲットをシミュレーション・テストに追加します。

10. 「攻撃に含めるシミュレーションの指定 (Which simulations do you want to include in the attack)」フィールドを使用して、含めるシミュレーションの横の **+** 記号を選択します。

    シミュレーション・オプションが**「次のシミュレーションを生成 (Generate a simulation where)」**ウィンドウに表示されます。

11. **「次のシミュレーションを生成 (Generate a simulation where)」**ウィンドウで、下線が付けられた任意のパラメーターをクリックして、シミュレーション・パラメーターをさらに構成します。

12. **「このシミュレーションの実行範囲 (Run this simulation for)」**ドロップダウン・リストで、このシミュレーションを実行するステップ数 (1 から 5) を選択します。

13. ステップのドロップダウン・リストで、シミュレーション実行のスケジュールを選択します。

14. グループ領域で、このシミュレーションを割り当てるグループのチェック・ボックスを選択します。

15. **「シミュレーションの保存 (Save Simulation)」**をクリックします。

シミュレーションの編集

シミュレーションを編集することができます。

手順

1. **「リスク」**タブをクリックします。

2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 編集するシミュレーション定義を選択します。
4. 「**アクション**」メニューから、「**編集**」を選択します。
5. 必要に応じて、パラメーターを更新します。

   シミュレーションのパラメーターについて詳しくは、シミュレーション・テストを参照してください。
6. 「**シミュレーションの保存 (Save Simulation)**」をクリックします。

シミュレーションの複製

シミュレーションを複製できます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. コピーするシミュレーションを選択します。
4. 「**アクション**」メニューから、「**コピー**」を選択します。
5. シミュレーションの名前を入力します。
6. 「**OK**」をクリックします。

シミュレーションの削除

シミュレーションを削除することができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 削除するシミュレーションを選択します。
4. 「**アクション**」メニューから、「**削除**」を選択します。
5. 「**OK**」をクリックします。

シミュレーションの手動実行

シミュレーション・エディターを使用して、シミュレーションを手動で実行します。

手順

1. 「**リスク**」タブをクリックします。
2. 「**アクション**」メニューから、「**シミュレーションの実行 (Run Simulation)**」を選択します。
3. 「**OK**」をクリックします。

タスクの結果

シミュレーション・プロセスは、長時間かかることがあります。シミュレーションの実行中は、「次の実行 (Next Run)」列に完了率が示されます。完了すると、「結果」列にシミュレーションの日時が表示されます。

シミュレーションを実行し、シミュレーションに関連するテストに影響を与える変更を実行すると、それらの変更は表示されるまでに最大で 1 時間かかる場合があります。

シミュレーション結果の管理

シミュレーションの実行後に、「結果」列には、シミュレーションが生成されたときの日付のリストが含まれるドロップダウン・リストが表示されます。

シミュレーション結果は 30 日間保持されます。結果は、シミュレーションが実行された後にのみ「結果」列に表示されます。

シミュレーション結果の表示

「シミュレーション」ページの「結果」列でシミュレーション結果を表示できます。

このタスクについて

結果は、シミュレーションが実行された後にのみ「結果」列に表示されます。シミュレーション結果は、シミュレーションの各ステップについての情報を提供します。

例えば、シミュレーションの最初のステップは、シミュレーションによって影響を受ける、直接接続されているアセットのリストを提供します。2 番目のステップは、シミュレーションの第 1 レベルのアセットと通信できる、ネットワーク内のアセットをリストします。

「結果の表示 (View Result)」をクリックすると、以下の情報が表示されます。

表 32. シミュレーション結果情報

パラメーター	説明
シミュレーション定義 (Simulation Definition)	シミュレーションの説明。
モデルの使用 (Using Model)	シミュレーションが実行された対象のモデルの名前。
シミュレーション結果 (Simulation Result)	シミュレーションが実行された日付。
ステップ結果数 (Step Results)	結果のステップの数 (現在表示されているステップを含む)。

表 32. シミュレーション結果情報 (続き)

パラメーター	説明
危殆化されたアセット数 (Assets Compromised)	このステップおよびすべてのシミュレーション・ステップで危殆化されたアセットの総数。 トポロジー・モデルに、到達可能として定義された /32 の IP 範囲からのデータが含まれる場合、IBM Security QRadar Risk Manager は、それらのアセットをデータベースに対して検証しません。したがって、それらのアセットは、「危殆化されたアセット数 (Asset Compromised)」の総数では考慮されません。QRadar Risk Manager は、/24 などのより広い IP 範囲のアセットのみを検証して、どのアセットが存在するかを判別します。
リスク・スコア	リスク・スコアは、結果の数、ステップの数、危殆化されたアセットの数、およびシミュレーションに割り当てられた重要度係数に基づいた計算値です。この値は、表示されたステップのシミュレーションに関連付けられている重大度レベルを示します。

接続の上にマウス・ポインターを移動すると、このシミュレーションによって影響を受けるアセットのリストを判別できます。

接続の上にマウスを移動すると、上位 10 件のアセットが表示されます。

接続の上にマウス・ポインターを移動すると、サブネットによって定義された、ネットワーク内のパスが強調表示されます。

シミュレーション結果ページには、「このステップの結果 (Results for this step)」という名前の表が表示されます。この表には、以下の情報が表示されます。

表 33. 「このステップの結果 (Results for this step)」情報

パラメーター	説明
承認 (Approve)	シミュレーション結果を承認できるようにします。『シミュレーション結果の承認』を参照してください。
親	シミュレーションの表示されたステップの発信元 IP アドレス。
IP	影響を受けるアセットの IP アドレス。
ネットワーク	ネットワーク階層内で定義された、ターゲット IP アドレスのネットワーク。
アセット名	アセット・プロファイルによって定義された、影響を受けるアセットの名前。
アセットの重み (Asset Weight)	アセット・プロファイル内で定義された、影響を受けるアセットの重み。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 「結果」列で、リストを使用して、表示するシミュレーションの日時を選択します。
4. 「**結果の表示 (View Result)**」をクリックします。シミュレーションのステップ 1 から開始して、シミュレーション結果情報を表示できます。
5. 「このステップの結果 (Results for this Step)」表を表示して、影響を受けるアセットを判別します。
6. シミュレーション結果の次のステップを表示するには、「**次のステップ (Next Step)**」をクリックします。

シミュレーション結果の承認

シミュレーション結果を承認することができます。

このタスクについて

アセットでの低リスクまたは通常の通信と見なすネットワーク・トラフィックを承認することができます。結果を承認するときには、結果リストをフィルターに掛け、その後のシミュレーションで通常または承認済みの通信を無視させます。

結果は、シミュレーションが実行された後にのみ「結果」列に表示されます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 「結果」列で、リストを使用して、表示するシミュレーションの日時を選択します。
4. 「**結果の表示 (View Result)**」をクリックします。
5. このステップ表の「結果」で、以下のいずれかの方法を使用してアセットを承認します。

オプション	説明
選択した項目を承認 (Approve Selected)	承認する各アセットのチェック・ボックスを選択してから、「**選択した項目を承認 (Approve Selected)**」をクリックします。
すべて承認 (Approve All)	クリックすると、リストされているアセットがすべて承認されます。

6. オプション。「**承認済みの表示 (View Approved)**」をクリックすると、承認済みのアセットがすべて表示されます。

シミュレーションの承認の取り消し

承認済みの接続または通信は、承認済みリストから取り除くことができます。承認済みのシミュレーション結果を削除すると、以降のシミュレーションでは、シミュレーション結果に非承認通信が表示されます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 「結果」列で、リストを使用して、表示するシミュレーションの日時を選択します。
4. **結果の表示 (View Result)**
5. 「**承認済みの表示 (View Approved)**」をクリックすると、承認済みのアセットがすべて表示されます。
6. 次のオプションのいずれかを選択してください。

オプション	説明
選択項目の取り消し (Revoke Selected)	取り消す各アセットのチェック・ボックスを選択して、「**選択項目の取り消し (Revoke Selected)**」をクリックします。
すべて取り消す (Revoke All)	リストされているすべてのアセットを取り消す場合にクリックします。

シミュレーションのモニター

シミュレーションの結果、変更が行われたかどうかを判別するために、シミュレーションをモニターできます。変更が行われると、イベントが生成されます。最大で 10 のシミュレーションをモニター・モードにすることができます。

このタスクについて

モニター・モードのシミュレーションの場合、デフォルトの時刻範囲は 1 時間です。この値は、シミュレーションの作成時に構成された時間値をオーバーライドします。

イベント・カテゴリーについて詳しくは、『*IBM Security QRadar SIEM ユーザーズ・ガイド*』を参照してください。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. モニターするシミュレーションを選択します。
4. 「**モニター**」をクリックします。
5. 「**イベント名**」フィールドに、「**ログ・アクティビティー**」タブと「**オフェンス**」タブに表示するイベントの名前を入力します。

6. 「**イベントの説明**」フィールドに、イベントの説明を入力します。この説明は、イベント詳細の「注釈」に表示されます。
7. 「**上位カテゴリー**」リストから、イベントの処理時にこのシミュレーションで使用する上位イベント・カテゴリーを選択します。
8. 「**下位カテゴリー**」リストから、イベントの処理時にこのシミュレーションで使用する下位イベント・カテゴリーを選択します。
9. このモニターされるシミュレーションの結果としてイベントを判定機能コンポーネントに転送する場合は、「**ディスパッチされたイベントをオフェンスの一部にする**」チェック・ボックスを選択します。オフェンスが生成されなかった場合は、新規オフェンスが作成されます。オフェンスが存在する場合、このイベントはその既存のオフェンスに追加されます。このチェック・ボックスを選択した場合は、次のいずれかのオプションを選択します。

オプション	説明
質問/シミュレーション (Question/Simulation)	質問からのすべてのイベントが、単一のオフェンスに関連付けられます。
アセット	固有のオフェンスが、固有のアセットごとに作成 (または更新) されます。

10. 「**追加のアクション (Additional Actions)**」セクションで、次の 1 つ以上のオプションを選択します。

オプション	説明
E メール	イベントが生成された場合に通知が送信されるようにするには、このチェック・ボックスを選択して、E メール・アドレスを指定します。複数の E メール・アドレスを指定する場合は、各アドレスをコンマで区切ってください。
Syslog に送信 (Send to Syslog)	イベントを記録するには、このチェック・ボックスを選択します。 例えば、syslog 出力の例を以下に示します。 `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: Eventdescription`
通知	このモニターされる質問の結果として生成されるイベントを、ダッシュボードの「システム通知」項目に表示する場合は、このチェック・ボックスを選択します。

11. 「**モニターを有効にする (Enable Monitor)**」セクションで、シミュレーションをモニターするチェック・ボックスを選択します。
12. 「**モニターの保存 (Save Monitor)**」をクリックします。

シミュレーションのグループ化

シミュレーションをグループに割り当てることは、すべてのシミュレーションを表示および追跡するための効率的な方法です。例えば、コンプライアンスに関連するすべてのシミュレーションを表示することができます。

このタスクについて

新規シミュレーションを作成する際に、そのシミュレーションを既存のグループに割り当てることができます。

グループを作成後、メニュー・ツリーでグループをドラッグして、編成を変更できます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 「**グループ (Groups)**」をクリックします。
4. メニュー・ツリーから、新しい下位グループを作成するグループを選択します。
5. 「**新規**」をクリックします。
6. 「**名前**」フィールドに、新規グループの名前を入力します。グループ名の長さは 255 文字までです。
7. 「**説明**」フィールドに、グループの説明を入力します。 説明の長さは 255 文字まで可能です。
8. 「**OK**」をクリックします。

グループの編集

グループを編集することができます。

このタスクについて

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 「**グループ (Groups)**」をクリックします。
4. メニュー・ツリーから、編集するグループを選択します。
5. 「**編集**」をクリックします。
6. 必要に応じて「名前」フィールドと「説明」フィールドの情報を更新します。
7. 「**OK**」をクリックします。

別のグループへの項目のコピー

グループ機能を使用して、シミュレーションを 1 つまたは多数のグループにコピーすることができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 「**グループ (Groups)**」をクリックします。

4. メニュー・ツリーから、別のグループにコピーする質問を選択します。
5. 「**コピー**」をクリックします。
6. シミュレーションのコピー先のグループのチェック・ボックスを選択します。
7. 「**コピー**」をクリックします。

グループからの項目の削除

項目をグループから削除することができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 「**グループ (Groups)**」をクリックします。
4. メニュー・ツリーから最上位グループを選択します。
5. グループのリストから、削除する項目またはグループを選択します。
6. 「**削除**」をクリックします。
7. 「**OK**」をクリックします。

項目のグループへの割り当て

シミュレーションをグループに割り当てることができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. グループに割り当てるシミュレーションを選択します。
4. 「**アクション**」メニューを使用して「**グループの割り当て**」を選択します。
5. 質問を割り当てるグループを選択します。
6. 「**グループの割り当て**」をクリックします。

第 14 章 トポロジー・モデル

既存のネットワークに基づく仮想ネットワーク・モデルを定義するためのトポロジー・モデルを使用できます。

組み合わせと構成が可能な一連の変更に基づいてネットワーク・モデルを作成できます。これにより、ネットワークを構成変更した場合の効果を、シミュレーションを使用して判断することができます。シミュレーションについて詳しくは、シミュレーションの使用を参照してください。

トポロジー・モデルは「シミュレーション」ページに表示できます。トポロジー・モデルには以下の情報が表示されます。

表 34. モデル定義のパラメーター

パラメーター	説明
モデル名 (Model Name)	トポロジー・モデルの名前。作成時にユーザーによって定義されたものです。
グループ	このトポロジーが関連付けられているグループ。
作成者	このモデル定義を作成したユーザー。
作成日時 (Created On)	このモデル定義が作成された日時。
最終変更日時	このモデル定義が作成されてからの経過日数。

トポロジー・モデルの作成

1 つ以上のトポロジー・モデルを作成できます。

© Copyright IBM Corp. 2012, 2015

このタスクについて

以下の表に、テスト名と構成可能なパラメーターを示します。

表 35. トポロジーのテスト

テスト名	パラメーター
送信元 CIDR から宛先 CIDR への接続を許可する選択したデバイスのプロトコル、ポートに関するルールを追加する (A rule is added to the selected devices that allows connections from source CIDRs to destination CIDRs on protocols, ports)	以下のパラメーターを構成します。 • **デバイス** - このルールを追加するデバイスを指定します。「パラメーターのカスタマイズ (Customize Parameter)」ウィンドウで、「すべて」チェック・ボックスを選択してすべてのデバイスを含めるか、以下の検索条件のいずれかを使用してデバイスを検索できます。 – **IP/CIDR** - 「IP/CIDR」オプションを選択し、このルールに追加する IP アドレスまたは CIDR を指定します。 – **ホスト名** - 「ホスト名」オプションを選択し、フィルタリングするホスト名を指定します。複数のホスト名を検索する場合は、ストリングの先頭または末尾にワイルドカード文字 (*) を使用します。 – **アダプター (Adapter)** - 「アダプター (Adapter)」オプションを選択し、ドロップダウン・リストを使用して、アダプターによりデバイス・リストをフィルタリングします。 – **ベンダー** - 「ベンダー」オプションを選択し、ドロップダウン・リストを使用して、ベンダーによりデバイス・リストをフィルタリングします。ベンダーのモデルを指定することもできます。複数のモデルを検索する場合は、ストリングの先頭または末尾にワイルドカード文字 (*) を使用します。 • **許可 (allows)	拒否 (denies)** - このテストで適用する、接続に対する条件 (受け入れまたは拒否) を選択します。 • **CIDR** - このルールを追加する任意の送信元 IP アドレスまたは CIDR 範囲を選択します。 • **CIDR** - このルールを追加する任意の宛先 IP アドレスまたは CIDR 範囲を選択します。 • **プロトコル** - このルールを追加するプロトコルを指定します。すべてのプロトコルを含めるには、「すべて」チェック・ボックスを選択します。 • **ポート** - このルールを追加するポートを指定します。すべてのポートを含めるには、「すべて」チェック・ボックスを選択します。

表 35. トポロジーのテスト (続き)

テスト名	パラメーター
送信元 CIDR から宛先 CIDR への接続を許可する、脆弱性のある選択した IPS デバイスにルールを追加する (A rule is added to the selected IPS devices that allows connections from source CIDRs to destination CIDRs with vulnerabilities)	以下のパラメーターを構成します。 • **IPS デバイス (IPS devices)** - このトポロジー・モデルに含める IPS デバイスを指定します。すべての IPS デバイスを含めるには、「すべて」チェック・ボックスを選択します。 • 許可 (allows) | 拒否 (denies) - このテストで適用する、接続に対する条件 (受け入れまたは拒否) を指定します。 • **CIDR** - このトポロジー・モデルに含める任意の送信元 IP アドレスまたは CIDR 範囲を指定します。 • **CIDR** - このトポロジー・モデルに含める任意の宛先 IP アドレスまたは CIDR 範囲を指定します。 • **脆弱性** - トポロジー・モデルに適用する脆弱性を指定します。Bugtraq ID、OSVDB ID、CVE ID、またはタイトルを使用して脆弱性を検索できます。
以下の資産は選択したポートへの接続を許可 (The following assets allow connections to the selected ports)	以下のパラメーターを構成します。 • アセット - このトポロジー・モデルに含めるアセットを指定します。 • **許可 (allow) | 拒否 (deny)** - このトポロジー・モデルで適用する、接続に対する条件 (受け入れまたは拒否) を指定します。デフォルトは許可 (allow) です。 • ポート - このトポロジー・モデルに含めるポートを指定します。すべてのポートを含めるには、「すべて」チェック・ボックスを選択します。
以下のアセット・ビルディング・ブロックのアセットはポートへの接続を許可	以下のパラメーターを構成します。 • アセット・ビルディング・ブロック - このトポロジー・モデルに含めるアセット・ビルディング・ブロックを指定します。 • **許可 (allow) | 拒否 (deny)** - このトポロジー・モデルで適用する条件 (受け入れまたは拒否) を指定します。デフォルトは許可 (allow) です。 • **ポート** - このトポロジー・モデルに含めるポートを指定します。すべてのポートを含めるには、「すべて」チェック・ボックスを選択します。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**トポロジー・モデル (Topology Models)**」を選択します。
3. 「**アクション**」メニューから、「新規」を選択します。
4. 「**このモデルの名前の指定 (What do you want to name this model)**」フィールドで、モデル定義の名前を入力します。

5. 「**モデルに適用する変更の指定 (Which modifications do you want to apply to your model)**」ペインで、モデルを作成するためにトポロジーに適用する変更を選択します。
6. 「**モデルを以下として構成 (Configure model as follows)**」ペインに追加されたテストを構成します。
7. テストがペイン内に表示されると、構成可能なパラメーターには下線が付けられます。各パラメーターをクリックして、モデルに対するこの変更をさらに構成します。「グループ」エリアで、チェック・ボックスを選択してこの質問にグループを割り当てます。
8. 「**モデルの保存 (Save Model)**」をクリックします。

トポロジー・モデルの編集

トポロジー・モデルを編集することができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**トポロジー・モデル (Topology Models)**」を選択します。
3. 編集するモデル定義を選択します。
4. 「**アクション**」メニューから、「編集」を選択します。
5. 必要に応じて、パラメーターを更新します。

   モデル・エディターのパラメーターについて詳しくは、トポロジー・モデルの作成を参照してください。
6. 「**モデルの保存 (Save Model)**」をクリックします。

トポロジー・モデルの複製

トポロジー・モデルを複製することができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**トポロジー・モデル (Topology Models)**」を選択します。
3. コピーするモデル定義を選択します。
4. 「**アクション**」メニューから、「**コピー**」を選択します。
5. コピーされたトポロジー・モデルに割り当てる名前を入力します。
6. 「**OK**」をクリックします。
7. モデルを編集します。

トポロジー・モデルの削除

トポロジー・モデルを削除することができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**トポロジー・モデル (Topology Models)**」を選択します。
3. 削除するモデル定義を選択します。
4. 「**アクション**」メニューから、「**削除**」を選択します。
5. 「**OK**」をクリックします。

トポロジー・モデルのグループ化

選択した条件に基づいて、トポロジー・モデルをグループ化したり表示したりできます。

トポロジー・モデルの分類は、効率的にモデルを表示して追跡するための方法です。例えば、コンプライアンスに関連するすべてのトポロジー・モデルを表示できます。

新規トポロジー・モデルを作成する際に、そのトポロジー・モデルを既存のグループに割り当てることができます。グループの割り当てについては、トポロジー・モデルの作成を参照してください。

グループの表示

グループを使用してトポロジー・モデルを表示できます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**トポロジー・モデル (Topology Models)**」を選択します。
3. 「**グループ**」リストを使用して、表示するグループを選択します。

グループの作成

グループを作成してトポロジー・モデルを効果的に表示および追跡できます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**トポロジー・モデル (Topology Models)**」を選択します。
3. 「**グループ (Groups)**」をクリックします。
4. メニュー・ツリーから、新しい下位グループを作成するグループを選択します。

   グループを作成した後、メニュー・ツリー項目でグループをドラッグ・アンド・ドロップして、編成を変更できます。
5. 「**新規**」をクリックします。
6. 新規グループに割り当てる名前を入力します。名前の長さは 255 文字まで可能です。
7. グループの説明を入力します。説明の長さは 255 文字まで可能です。

8. 「**OK**」をクリックします。
9. 新しいグループの場所を変更するには、新しいグループをクリックし、メニュー・ツリー内の場所にフォルダーをドラッグします。

グループの編集

グループを編集することができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**トポロジー・モデル (Topology Models)**」を選択します。
3. 「**グループ (Groups)**」をクリックします。
4. メニュー・ツリーから、編集するグループを選択します。
5. 「**編集**」をクリックします。
6. パラメーターの値を更新します。
7. 「**OK**」をクリックします。
8. グループの場所を変更するには、新しいグループをクリックし、メニュー・ツリー内の場所にフォルダーをドラッグします。

別のグループへの項目のコピー

グループ機能を使用して、トポロジー・モデルを 1 つまたは多数のグループにコピーすることができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**トポロジー・モデル (Topology Models)**」を選択します。
3. 「**グループ (Groups)**」をクリックします。
4. メニュー・ツリーから、別のグループにコピーする質問を選択します。
5. 「**コピー**」をクリックします。
6. シミュレーションのコピー先のグループのチェック・ボックスを選択します。
7. 「**コピー**」をクリックします。

グループからの項目の削除

項目をグループから削除することができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. 「**グループ (Groups)**」をクリックします。
4. メニュー・ツリーから最上位グループを選択します。
5. グループのリストから、削除する項目またはグループを選択します。

6. 「**削除**」をクリックします。
7. 「**OK**」をクリックします。

トポロジーのグループへの割り当て

トポロジー・モデルをグループに割り当てることができます。

手順

1. 「**リスク**」タブをクリックします。
2. ナビゲーション・メニューで、「**シミュレーション**」 > 「**シミュレーション**」を選択します。
3. グループに割り当てるトポロジー・モデルを選択します。
4. 「**アクション**」メニューから、「**グループの割り当て**」を選択します。
5. 質問を割り当てるグループを選択します。
6. 「**グループの割り当て**」をクリックします。

第 15 章 監査ログ・データ

IBM Security QRadar Risk Manager ユーザーにより行われた変更は、IBM Security QRadar SIEM の「**ログ・アクティビティー**」タブに記録されます。

すべてのログは、「リスク・マネージャー監査」カテゴリーに表示されます。QRadar SIEM の「**ログ・アクティビティー**」タブの使用について詳しくは、「*IBM Security QRadar SIEM ユーザーズ・ガイド*」を参照してください。

ログに記録されるアクション

コンポーネントのアクションがログに記録されます。

以下の表に、ログに記録されるカテゴリーおよび対応するアクションをリストします。

表 36. ログに記録されるアクション

カテゴリー	アクション
ポリシー・モニター	質問を作成する。
	質問を編集する。
	質問を削除する。
	質問を手動で送信する。
	質問を自動で送信する。
	結果を承認する。
	結果の承認を取り消す。
トポロジー・モデル	トポロジー・モデルを作成する。
	トポロジー・モデルを編集する。
	トポロジー・モデルを削除する。
トポロジー	レイアウトを保存する。
	トポロジーの保存済み検索を作成する。
	トポロジーの保存済み検索を編集する。
	トポロジーの保存済み検索を削除する。
	IPS を配置する。
構成モニター	ログ・ソース・マッピングを作成する。
	ログ・ソース・マッピングを編集する。
	ログ・ソース・マッピングを削除する。
シミュレーション	シミュレーションを作成する。
	シミュレーションを編集する。
	シミュレーションを削除する。
	シミュレーションを手動で実行する。
	シミュレーションを自動で実行する。
	シミュレーションの結果を承認する。
	シミュレーションの結果を取り消す。

© Copyright IBM Corp. 2012, 2015

表 36. ログに記録されるアクション (続き)

カテゴリー	アクション
構成ソース管理	セッションで初めて認証に成功する。
	デバイスを追加する。
	デバイスを削除する。
	デバイスの IP アドレスまたはアダプターを編集する。
	資格情報構成を保存する。
	資格情報構成を削除する。
	プロトコル構成を保存する。
	プロトコル構成を削除する。
	バックアップ・ジョブのスケジュールを作成する。
	バックアップ・ジョブのスケジュールを削除する。
	バックアップ・ジョブを編集する。
	バックアップ・ジョブを追加する。
	バックアップ・ジョブを削除する。
	スケジュール済みバックアップ・ジョブを実行する。
	スケジュール済みジョブを、成功または失敗に関わらず、完了する。
	バックアップ・ジョブの処理が完了し、構成が保持された後、変更内容が検出されなかった。
	バックアップ・ジョブの処理が完了し、構成が保持された後、変更内容が検出された。
	バックアップ・ジョブの処理が完了し、構成が保持された後、保持されていない変更内容が検出された。
	バックアップ・ジョブの処理が完了した後、前に保持された構成がデバイスに存在しなくなった。
	プロトコルと資格情報を含む、アダプター操作の試行が開始された。
	プロトコルと資格情報を含む、アダプター操作の試行が成功した。

ユーザー・アクティビティーの表示

IBM Security QRadar Risk Manager ユーザーのユーザー・アクティビティーを表示できます。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。以前に検索をデフォルトとして保存した場合は、その保存済み検索の結果が表示されます。
2. 「**検索**」 > 「**新規検索**」をクリックして、検索を作成します。
3. 「**時刻範囲**」ペインで、この検索用にキャプチャーする時刻範囲のオプションを選択します。
4. 「**検索パラメーター**」ペインで、以下のように検索条件を定義します。
   a. 最初のリストから「**カテゴリー**」を選択します。
   b. 「**上位カテゴリー**」ドロップダウン・リストから、「**リスク・マネージャー監査**」を選択します。
   c. オプション。「**下位カテゴリー**」ドロップダウン・リストから、カテゴリーを選択して、検索を詳細化します。
5. 「**フィルターの追加**」をクリックします。
6. 「**フィルター**」をクリックして、QRadar Risk Manager イベントを検索します。

ログ・ファイルの表示

監査ログは、プレーン・テキストで保管され、監査ログ・ファイルが 200 MB のサイズに達するとアーカイブおよび圧縮されます。

このタスクについて

現行のログ・ファイルの名前は audit.log です。監査ログ・ファイルが 2 回目に 200 MB のサイズに達すると、ファイルが圧縮され、古い監査ログの名前は audit.1.gz に変更されます。 ログ・ファイルがアーカイブされるたびに、ファイル名の番号が 1 ずつ増えていきます。IBM Security QRadar Risk Manager には、最大で 50 個のアーカイブ・ログ・ファイルを保管することができます。

監査メッセージ (日付、時刻、ホスト名は含まない) の最大サイズは 1024 文字です。

ログ・ファイルの各エントリーは以下の形式を使用して表示されます。

```
<date_time> <host name> <user>@<IP address>
(thread ID) [<category>] [<sub-category>]
[<action>] <payload>
```

以下の表では、ログ・ファイルで使用されるパラメーターについて説明します。

表 37. 監査ログ・ファイル情報

パラメーター	説明
<date_time>	Month Date HH:MM:SS 形式のアクティビティーの日時。
<host name>	このアクティビティーがログに記録されたコンソールのホスト名。
<user>	アクションを実行したユーザーの名前。
<IP address>	アクションを実行したユーザーの IP アドレス。

表 37. 監査ログ・ファイル情報 (続き)

パラメーター	説明
(thread ID)	このアクティビティーをログに記録した Java™ スレッドの ID。
<category>	このアクティビティーの上位カテゴリー。
<sub-category>	このアクティビティーの下位カテゴリー。
<action>	発生したアクティビティー。
<payload>	変更された完全なレコード (ある場合)。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar SIEM コンソールにログインします。
2. IBM Security QRadar SIEM コンソールから SSH を使用して、root ユーザーとして QRadar Risk Manager アプライアンスにログインします。
3. 以下のディレクトリーに移動します。`/var/log/audit`
4. 監査ログ・ファイルを開きます。

ログ・ファイルの詳細

管理者は、IBM Security QRadar Risk Manager ログ・ファイルを使用して、ユーザー・アクティビティーを表示したりシステムの問題をトラブルシューティングしたりします。

QRadar Risk Manager ログ・ファイルの場所と内容について以下の表で説明します。

表 38. QRadar Risk Manager ログ・ファイル

ログ・ファイル名	ロケーション	説明
`audit.log`	`/var/log/audit/`	現在の監査情報を含みます。
`audit.<1-50>.gz`	`/var/log/audit/`	アーカイブされた監査情報を含みます。`audit.log` ファイルのサイズが 200MB に達すると、圧縮されて `audit.1.gz` に名前変更されます。ログ・ファイルがアーカイブされるたびに、ファイル名の番号が 1 ずつ増えていきます。QRadar Risk Manager には、最大で 50 個のアーカイブ・ログ・ファイルを保管することができます。
`qradar.log`	`/var/log/`	QRadar Risk Manager サーバーによって記録されたすべてのプロセス情報を含みます。
`qradar.error`	`/var/log/`	このファイルには、QRadar Risk Manager サーバーによって生成されたすべての例外、`System.out` メッセージ、および `System.err` メッセージが記録されます。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

© Copyright IBM Corp. 2012, 2015

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項をご確認ください。

このソフトウェア・オファリングは、展開される構成に応じて、セッション管理および認証の目的のために、それぞれのお客様のセッション ID を、セッションごとの Cookie を使用して収集する場合があります。これらの Cookie は無効にできますが、その場合、これらを有効にした場合の機能を活用することはできません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

用語集

この用語集には、IBM Security QRadar Risk Manager のソフトウェアと製品で使用される用語と定義が記載されています。

この用語集では、以下の相互リファレンスを使用しています。

- 「～を参照」という表現は、非優先用語の場合は優先用語を参照し、略語の場合は正式な用語を参照するように促すための表現です。
- 「～も参照」という表現は、関連する用語や対比的な用語を参照するように促すための表現です。

この用語集に記載されていない用語と定義については、IBM Terminology Web サイト (新しいウィンドウで開きます) を参照してください。

『A』 『C』 『M』 『N』 180 ページの『R』 180 ページの『S』 180 ページの『T』 180 ページの『V』

A

アダプター (adapter)
2 つの異なるソフトウェア・コンポーネントが相互通信するための仲介ソフトウェア・コンポーネント。

アセット (asset)
稼働環境にデプロイされているか、デプロイされる予定の管理可能オブジェクト。

アセット・テスト (asset test)
潜在的なリスクのインディケーターを識別するために使用されるテスト。ネットワーク上のアセットが定義済みのポリシーに違反している場合や、現在の環境にリスクをもたらす場合、このテストによって通知される。

攻撃 (attack)
許可されていない人物がソフトウェア・プログラムやネットワーク・システムの操作を侵害しようとする行為。

攻撃パス (attack path)
攻撃に関連するソース、宛先、およびデバイス。

属性 (attribute)
コンポーネントに関連付けられているデータ。例えば、サーバー・コンポーネントに関連する属性としては、ホスト名、IP アドレス、ハード・ディスクの数などがある。

C

接続グラフ (connection graph)
リモート・ネットワーク・ノードとローカル IP アドレスからローカル・ネットワーク・ノードへの接続を示すグラフ。

接続線 (connection line)
接続グラフ上の、リモート・ネットワーク・ノードとローカル・ネットワーク・ノード間の線、または 2 つのローカル・ネットワーク・ノード間の線。

寄与テスト (contributing test)
質問で指定されたリスク・インディケーターを調べるテスト。

M

複数コンテキスト・デバイス (multiple-context device)
複数の仮想デバイスに分割された単一のアプライアンス。それぞれの仮想デバイスは、独立したデバイスとして独自のセキュリティー・ポリシーを持つ。

N

NAT
ネットワーク・アドレス変換 (Network Address Translation) を参照。

NAT インディケーター (NAT indicator)
2 つのネットワーク接続間のパスにソースまたは宛先のアドレス変換が含まれていることを示すトポロジー・グラフ上のインディケーター。

© Copyright IBM Corp. 2012, 2015

隣接データ (neighbor data)
QRadar Quality Manager の管理対象ホストに接続されているデバイスに関する情報を検出するために使用される、アダプターから収集された情報。

ネットワーク・アドレス変換 (NAT) (Network Address Translation (NAT))
ファイアウォールにおいて、セキュアなインターネット・プロトコル (IP) アドレスを外部の登録済みアドレスに変換すること。これにより、外部ネットワークとの通信が可能になり、ファイアウォール内部で使用される IP アドレスはマスクされる。

R

制限テスト (restrictive test)
寄与テストの質問で返された結果をフィルタリングするテスト。

リスク・インディケーター (risk indicator)
システムがセキュリティー違反にさらされる可能性を示す指標。

危険なプロトコル (risky protocol)
インターネットから DMZ へのインバウンド通信において、開いているポートで実行されるサービスに関連付けられたプロトコル。

ルール (rule)
コンピューター・システムが関係を識別し、それに応じて、自動化された応答を実行できるようにする一連の条件ステートメント。

S

サブ検索 (sub-search)
完了した検索結果セット内での検索照会の実行を可能にする機能。

T

時系列グラフ (time series chart)
ネットワーク接続の経時的変化をグラフィカル表現で示したグラフ。

トポロジー・グラフ (topology graph)
サブネット、デバイス、ファイアウォールを示すグラフ。

トポロジー・モデル (topology model)
ネットワーク・アセットの配置の仮想表現。攻撃のシミュレーションに使用される。

V

違反 (violation)
企業のポリシーをバイパスする行為、または企業のポリシーに違反する行為。

脆弱性 (vulnerability)
オペレーティング・システム、システム・ソフトウェア、またはアプリケーション・ソフトウェア・コンポーネントでの機密漏れ。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

© Copyright IBM Corp. 2012, 2015