IBM Security QRadar SIEM
バージョン 7.2.4

スタートアップ・ガイド

お願い

本書および本書で紹介する製品をご使用になる前に、 25 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。

本書は、本書の更新版に置き換えられない限り、IBM QRadar Security Intelligence Platform V7.2.4 および以降のリリースに適用されます。

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 SIEM
Version 7.2.4
Getting Started 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

目次

QRadar SIEM スタートアップ・ガイドについて

「IBM Security QRadar® SIEM スタートアップ・ガイド」では、主要な概念、インストール・プロセスの概要、およびユーザー・インターフェースで行う基本タスクについて説明します。

対象読者

本書の情報は、ネットワーク・セキュリティーの調査および管理を担当するセキュリティー管理者による使用を対象としています。本ガイドを使用するにあたっては、企業ネットワーク・インフラストラクチャーおよびネットワーキング・テクノロジーに関する知識が必要です。

技術文書

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 QRadar documentation (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 for IBM Security QRadar (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 システムのセキュリティーでは、企業の内部と外部からの不正なアクセスの防止、検出、対応により、システムと情報を保護する必要があります。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、合法かつ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。

Please Note:

本プログラムの利用は、様々な法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。IBM Security QRadar は、合法的な目的のために合法的な手段を用いてのみ使用することができます。お客様は、適用される法律、規制、およびポリシーに従って本プログラムを使用することに同意し、かかる法律、規制、およびポ

リシーを遵守する全責任を負うものとします。ライセンシーは、IBM Security QRadar の合法的な使用に必要なすべての同意、許可、または使用権を取得するか、取得済みであることを表明するものとします。

第 1 章 QRadar SIEM の概要

IBM Security QRadar SIEM は、状況認識およびコンプライアンス・サポートを提供するネットワーク・セキュリティー管理プラットフォームです。QRadar SIEM では、フロー・ベースのネットワーク知識、セキュリティー・イベント相関、およびアセット・ベースの脆弱性評価を組み合わせて使用します。

使用を開始するには、基本の QRadar SIEM インストール済み環境を構成し、イベントおよびフロー・データを収集し、レポートを生成します。

ログ・アクティビティー

IBM Security QRadar SIEM では、ネットワーク・イベントをリアルタイムでモニターおよび表示したり、拡張検索を実行したりできます。

「**ログ・アクティビティー**」タブには、ログ・ソース (ファイアウォールやルーター・デバイスなど) からのレコードとしてイベント情報が表示されます。「**ログ・アクティビティー**」タブを使用して、以下の作業を実行できます。

- イベント・データを調査する。
- QRadar SIEM に送信されるイベント・ログをリアルタイムで調査する。
- イベントを検索する。
- 構成可能な時系列グラフを使用してログ・アクティビティーをモニターする。
- フォールス・ポジティブを識別して QRadar SIEM をチューニングする。

ネットワーク・アクティビティー

IBM Security QRadar SIEM では、2 つのホスト間の通信セッションを調査できます。

「**ネットワーク・アクティビティー**」タブには、ネットワーク・トラフィックの通信方法に関する情報、また、コンテンツ・キャプチャー・オプションが有効になっている場合にはその通信内容が表示されます。「**ネットワーク・アクティビティー**」タブを使用して、以下の作業を実行できます。

- QRadar SIEM に送信されるフローをリアルタイムで調査する。
- ネットワーク・フローを検索する。
- 構成可能な時系列グラフを使用してネットワーク・アクティビティーをモニターする。

アセット

QRadar SIEM では、パッシブ・フロー・データおよび脆弱性データを使用してネットワーク・サーバーおよびホストをディスカバーすることにより、アセット・プロファイルを自動的に作成します。

アセット・プロファイルは、ネットワーク内の既知の各アセット (実行中のサービスを含む) に関する情報を提供します。アセット・プロファイル情報は相関の目的で使用され、フォールス・ポジティブを低減するために役立ちます。

「アセット」タブを使用して、以下の作業を実行できます。

- アセットを検索する。
- 学習済みのアセットをすべて表示する。
- 学習済みのアセットのアイデンティティー情報を表示する。
- フォールス・ポジティブ脆弱性をチューニングする。

オフェンス

IBM Security QRadar SIEM では、オフェンスを調査して、ネットワークの問題の根本原因を判別できます。

「**オフェンス**」タブを使用して、ネットワーク上で発生しているすべてのオフェンスを表示し、以下の作業を実行できます。

- オフェンス、送信元および宛先 IP アドレス、ネットワーク振る舞い、およびネットワーク上のアノマリを調査する。
- 複数のネットワークの発信元から同じ宛先 IP アドレスへのイベントおよびフローを相関付ける。
- 「**オフェンス**」タブのさまざまなページをナビゲートして、イベントおよびフローの詳細を調査する。
- オフェンスの原因となった固有のイベントを判別する。

レポート

IBM Security QRadar SIEM では、カスタム・レポートを作成するか、またはデフォルト・レポートを使用することができます。

QRadar SIEM が提供するデフォルトのレポート・テンプレートを、カスタマイズしてブランドを付け直し、QRadar SIEM ユーザーに配布することができます。

レポート・テンプレートは、コンプライアンス・レポート、デバイス・レポート、エグゼクティブ・レポート、ネットワーク・レポートなどのレポート・タイプにグループ化されています。「**レポート**」タブを使用して、以下の作業を実行します。

- QRadar SIEM データのレポートを作成、配布、および管理する。
- 運用での使用およびエグゼクティブの使用のためのカスタマイズされたレポートを作成する。
- セキュリティー情報とネットワーク情報を 1 つのレポートに結合する。
- 事前インストール済みのレポート・テンプレートを使用または編集する。
- カスタマイズされたロゴでレポートをブランド付けする。ブランド付けは、レポートをさまざまな対象者に配布する際に役立ちます。
- カスタム・レポートおよびデフォルト・レポート両方を生成するスケジュールを設定する。
- レポートを各種フォーマットで公開する。

データ収集

QRadar SIEM は、セキュリティー・イベント、ネットワーク・トラフィック、スキャン結果を含む、さまざまな形式の情報を多様なデバイスから受け入れます。

収集されたデータは、イベント、フロー、および脆弱性評価情報の 3 つの大きなセクションに分類されます。

イベント・データ収集

イベントは、ファイアウォール、ルーター、サーバー、および侵入検知システム (IDS) または侵入防止システム (IPS) などのログ・ソースにより生成されます。

ほとんどのログ・ソースは、syslog プロトコルを使用して QRadar SIEM に情報を送信します。QRadar SIEM では、以下のプロトコルもサポートしています。

- Simple Network Management Protocol (SNMP)
- Java™ Database Connectivity (JDBC)
- Security Device Event Exchange (SDEE)

デフォルトでは、一定の時間フレーム内に特定の数の識別可能なログを受信すると、QRadar SIEM は自動的にログ・ソースを検出します。ログ・ソースが正常に検出されると、QRadar SIEM により、適切なデバイス・サポート・モジュール (DSM) が「**管理**」タブ内の「ログ・ソース」ウィンドウに追加されます。

ほとんどの DSM にはネイティブのログ送信機能が組み込まれていますが、いくつかの DSM では、ログを送信するために追加構成またはエージェント、あるいはその両方が必要になります。構成は DSM タイプによって異なります。DSM が、QRadar SIEM がサポートする形式でログを送信するように構成する必要があります。 DSM の構成について詳しくは、「*DSM Configuration Guide*」を参照してください。

ルーターやスイッチなどの特定のログ・ソース・タイプでは、QRadar SIEM がそれらを素早く検出して「ログ・ソース」リストに追加するだけの十分なログが送信されません。これらのログ・ソースは手動で追加できます。ログ・ソースの手動での追加について詳しくは、「*Log Sources User Guide*」を参照してください。

収集されたデータは、イベント、フロー、および脆弱性評価 (VA) 情報の 3 つの大きなセクションに分類されます。

フロー・データ収集

フローによりネットワーク・トラフィックに関する情報が提供されます。フローは、Flowlog ファイル、NetFlow、J-Flow、sFlow、Packeteer などのさまざまなフォーマットで QRadar SIEM に送信できます。

複数のフロー・フォーマットを同時に受け入れることで、QRadar SIEM では、情報の収集をイベントだけに依存していた場合には見逃す可能性がある脅威やアクティビティーを検出することが可能です。

QRadar QFlow Collector は、アプリケーションが作動しているポートにかかわらず、ネットワーク・トラフィックの完全なアプリケーション検出を提供します。例

えば、Internet Relay Chat (IRC) プロトコルがポート 7500/TCP で通信している場合、QRadar QFlow Collector はこのトラフィックを IRC として識別し、会話の開始のパケット・キャプチャーを提供します。NetFlow および J-Flow は、ポート 7500/TCP 上にトラフィックが存在することを通知するだけであり、使用されているプロトコルに関するコンテキストは提供しません。

一般的なミラー・ポートのロケーションにはコア、DMZ、サーバー、アプリケーション・スイッチなどがあり、NetFlow はボーダー・ルーターおよびボーダー・スイッチからの補足情報を提供します。

QRadar QFlow Collector はデフォルトで使用可能になっており、QRadar SIEM アプライアンスの使用可能なインターフェースに、ミラー、SPAN、または TAP を接続する必要があります。ミラー・ポートが QRadar SIEM アプライアンスのいずれかのネットワーク・インターフェースに接続されると、フロー分析が自動的に開始されます。デフォルトでは、QRadar SIEM は、管理インターフェース上でポート 2055/UDP の NetFlow トラフィックをモニターします。必要に応じて、追加の NetFlow ポートを割り当てることができます。

脆弱性評価情報

QRadar SIEM では、各種サード・パーティー・スキャナーから VA 情報をインポートできます。

VA 情報は、QRadar Risk Manager が、アクティブなホスト、オープン・ポート、および潜在的な脆弱性を識別するのに役立ちます。

QRadar Risk Manager は、VA 情報を使用して、ネットワーク上のオフェンスのマグニチュードをランク付けします。

VA スキャナーのタイプによっては、QRadar Risk Manager は、スキャナー・サーバーからスキャン結果をインポートしたり、スキャンをリモート側で開始したりすることができます。

QRadar SIEM のルール

ルールは、イベント、フロー、またはオフェンスに対してテストを実行し、すべてのテスト条件が満たされた場合に応答を生成します。

QRadar SIEM には、過度なファイアウォールでの拒否、複数のログイン試行失敗、潜在的なボットネット・アクティビティーなど、広範囲のアクティビティーを検出するルールが備わっています。ルールについて詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

以下のリストで、2 つのルール・カテゴリーについて説明します。

- カスタム・ルールは、イベント、フロー、およびオフェンスに対してテストを実行し、ネットワーク内の異常なアクティビティーを検出します。
- アノマリ検出ルールは、ネットワークで異常なトラフィック・パターンが発生したときにそれを検出するために、保存済みのフローまたはイベント検索の結果に対してテストを実行します。

重要: 管理アクセス権限を持たないユーザーは、自分がアクセス可能なネットワークの領域に対するルールを作成できます。ルールを管理するには、適切なロール権限を所持している必要があります。ユーザー・ロール権限について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

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、サポート対象の 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	**サポート対象バージョン**
Mozilla Firefox	17.0 延長サポート版 24.0 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)	9.0 10
Google Chrome	IBM Security QRadar V7.2.4 製品のリリース日時点での現行バージョン

第 2 章 QRadar SIEM デプロイメントの開始

IBM Security QRadar SIEM の主要機能を評価する前に、管理者は QRadar SIEM をデプロイする必要があります。

QRadar SIEM をデプロイするには、管理者は以下の作業を実行する必要があります。

- QRadar SIEM アプライアンスをインストールする。
- QRadar SIEM インストール済み環境を構成する。
- イベント、フロー、および脆弱性評価 (VA) データを収集する。
- QRadar SIEM インストール済み環境をチューニングする。

QRadar SIEM アプライアンスのインストール

管理者は QRadar SIEM アプライアンスをインストールして、ユーザー・インターフェースへのアクセスを使用可能にする必要があります。

始める前に

QRadar SIEM 評価アプライアンスをインストールする前に、以下を確認してください。

- 2 ユニット・アプライアンス用のスペース。
- ラック・レールおよびシェルフ (マウント)。
- (オプション) コンソール・アクセス用の USB キーボードおよび標準 VGA モニター。

手順

1. 管理ネットワーク・インターフェースを、Ethernet 1 とラベルが付けられたポートに接続します。
2. 専用の電源接続をアプライアンスの背面に接続します。
3. コンソール・アクセスが必要な場合、USB キーボードおよび標準 VGA モニターを接続します。
4. アプライアンスにフロント・パネルがある場合、両側のつまみを押してからパネルを引くことにより、アプライアンスからパネルを取り外します。
5. アプライアンスの電源をオンにします。

QRadar SIEM アプライアンス

QRadar SIEM 評価アプライアンスは、2 ユニットのラック・マウント・サーバーです。評価機器には、ラック・レールまたはシェルフは付属していません。

QRadar SIEM アプライアンスには、4 つのネットワーク・インターフェースが組み込まれています。この評価では、Ethernet 1 とラベルが付けられたインターフェースを管理インターフェースとして使用します。

残りの 3 つのモニター・インターフェースを、フロー収集に使用できます。QRadar QFlow Collector は、完全なネットワーク・アプリケーション分析を提供しており、各会話の開始時にパケット・キャプチャーを実行できます。QRadar SIEM アプライアンスによっては、SPAN ポートまたは TAP が Ethernet 1 以外のインターフェースに接続されると、フロー分析が自動的に開始されます。QRadar SIEM 内の QRadar QFlow Collector コンポーネントを有効にするために追加の手順が必要になる場合があります。

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。

制約事項: QRadar SIEM 評価アプライアンスのフロー分析では、50 Mbps の制限があります。フロー収集用のモニター・インターフェースの総トラフィックが 50 Mbps を超えないようにしてください。

QRadar SIEM の構成

QRadar SIEM を構成することにより、ネットワーク階層をレビューし、自動更新をカスタマイズすることができます。

手順

1. QRadar 製品ユーザー・インターフェースにアクセスするために使用するすべてのデスクトップ・システムに、以下のアプリケーションがインストールされていることを確認してください。
   - Java ランタイム環境 (JRE) バージョン 1.7 または IBM 64-bit Runtime Environment for Java V7.0
   - Adobe Flash バージョン 10.x
2. サポート対象の Web ブラウザーを使用していることを確認します。 5 ページの『サポート対象の Web ブラウザー』を参照してください。
3. Internet Explorer を使用する場合、ドキュメント・モードおよびブラウザー・モードを有効にしてください。
   a. 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。
   b. 「**ブラウザー モード**」をクリックして、Web ブラウザーのバージョンを選択します。
   c. 「**ドキュメント モード**」をクリックして、「**IE7 標準**」を選択します。
4. 以下の URL を入力して QRadar SIEM ユーザー・インターフェースにログインします。

   https://<IP Address>

   ここで、<IP Address> は QRadar SIEM Console の IP アドレスです。

ネットワーク階層

業務ごとに編成されたネットワークのさまざまな領域を表示し、ビジネス・バリューのリスクに従って脅威およびポリシー情報の優先順位付けを行うことができます。

QRadar SIEM では、以下の作業を実行するためにネットワーク階層を使用します。

- ネットワーク・トラフィックを理解し、ネットワーク・アクティビティーを表示する。
- ネットワーク内の特定の論理グループまたはサービス (マーケティング、DMZ、VoIP など) をモニターする。
- トラフィックをモニターし、各グループおよびグループ内のホストの振る舞いのプロファイルを作成する。
- ローカル・ホストおよびリモート・ホストを判定して識別する。

評価のために、事前定義された論理グループを含むデフォルトのネットワーク階層が提供されています。ネットワーク階層が正確かつ完全であることを確認してください。ご使用の環境に、事前構成されたネットワーク階層に表示されないネットワーク範囲が含まれている場合、それらを手動で追加する必要があります。

ネットワーク階層に定義されるオブジェクトは、環境内に物理的に存在しているものだけではありません。インフラストラクチャーに属するすべての論理ネットワーク範囲を、ネットワーク・オブジェクトとして定義する必要があります。

注: システムに完成したネットワーク階層が組み込まれていない場合、「**管理**」タブを使用してご使用の環境に固有の階層を作成してください。

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。

ネットワーク階層のレビュー

ネットワーク階層をレビューできます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・ペインで、「**システム構成**」をクリックします。
3. 「**ネットワーク階層**」アイコンをクリックします。
4. 「**グループの管理: 上位 (Manage Group:Top)**」リストで、「**Regulatory_Compliance_Servers**」をクリックします。

   ネットワーク階層に規制コンプライアンス・サーバー・コンポーネントが含まれていない場合、この手順の残りではメール・コンポーネントを使用できます。
5. 「**このオブジェクトの編集 (Edit this object)**」アイコンをクリックします。
6. コンプライアンス・サーバーを追加するには、以下のようにします。
   a. 「**IP/CIDR**」フィールドに、コンプライアンス・サーバーの IP アドレスまたは CIDR 範囲を入力します。
   b. 「**追加**」をクリックします。
   c. すべてのコンプライアンス・サーバーについて繰り返します。
   d. 「**保存**」をクリックします。
   e. 編集するその他のネットワークすべてに対してこの手順を繰り返します。
7. 「**管理**」タブ・メニューで、「**変更のデプロイ**」をクリックします。

最新のネットワーク・セキュリティー情報を使用して、自動または手動で構成ファイルを更新できます。QRadar SIEM では、システム構成ファイルを使用して、ネットワーク・データ・フローの役に立つ特性を提供します。

自動更新

更新を受信するには、QRadar SIEM コンソールがインターネットに接続されている必要があります。コンソールがインターネットに接続されていない場合、内部更新サーバーを構成する必要があります。

自動更新サーバーのセットアップについては、「*IBM Security QRadar SIEM ユーザーズ・ガイド*」を参照してください。

QRadar SIEM を使用して、既存の構成ファイルを置き換えるか、または更新ファイルを既存のファイルと統合することができます。

ソフトウェア更新は、以下の Web サイトからダウンロードできます。

http://www.ibm.com/support/fixcentral/

更新ファイルには、以下の更新が含まれる可能性があります。

- 構成の更新。これには、構成ファイルの変更、脆弱性、QID マップ、およびセキュリティー脅威情報の更新が含まれます。
- DSM 更新。これには、構文解析の問題の修正、スキャナーの変更、およびプロトコル更新が含まれます。
- メジャー更新。これには、更新された JAR ファイルなどの項目が含まれます。
- マイナー更新。これには、追加のオンライン・ヘルプ・コンテンツや更新されたスクリプトなどの項目が含まれます。

自動更新設定の構成

QRadar SIEM 更新の頻度、更新タイプ、サーバー構成、およびバックアップ設定をカスタマイズできます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・ペインで、「**システム構成**」をクリックします。
3. 「**自動更新**」アイコンをクリックします。
4. ナビゲーション・ペインで、「**設定の変更**」をクリックします。
5. 「**自動更新スケジュール**」ペインで、デフォルト・パラメーターを受け入れます。
6. 「**更新タイプ**」ペインで、以下のパラメーターを構成します。
   a. 「**構成の更新**」リスト・ボックスで、「**自動更新**」を選択します。
   b. 以下のパラメーターについてはデフォルト値を受け入れます。
      - DSM、スキャナー、プロトコルの更新。
      - メジャー更新。
      - マイナー更新。
7. 「**自動デプロイ**」チェック・ボックスをクリアします。

デフォルトでは、このチェック・ボックスは選択されています。このチェック・ボックスが選択されていない場合、システム通知が「**ダッシュボード**」タブに表示され、更新のインストール後に変更をデプロイする必要があることが示されます。

8. 「**拡張**」タブをクリックします。
9. 「**サーバー構成**」ペインで、デフォルト・パラメーターを受け入れます。
10. 「**その他の設定**」ペインで、デフォルト・パラメーターを受け入れます。
11. 「**保存**」をクリックして「更新」ウィンドウを閉じます。
12. ツールバーの「**変更のデプロイ**」をクリックします。

イベントの収集

イベントを収集することにより、リアルタイムで QRadar SIEM に送信されるログを調査できます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・ペインで、「**データ・ソース**」をクリックします。
3. 「**ログ・ソース**」アイコンをクリックします。
4. ログ・ソースのリストをレビューし、ログ・ソースを必要に応じて変更します。

   ログ・ソースの構成について詳しくは、「*Log Sources User Guide*」を参照してください。
5. 「ログ・ソース」ウィンドウを閉じます。
6. 「**管理**」タブ・メニューで、「**変更のデプロイ**」をクリックします。

フローの収集

フローを収集することにより、ホスト間のネットワーク通信セッションを調査できます。

サード・パーティーのネットワーク・デバイス上 (スイッチやルーターなど) でフローを有効にする方法について詳しくは、ベンダーの資料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、「**データ・ソース**」 > 「**フロー**」をクリックします。
3. 「**フロー・ソース**」アイコンをクリックします。
4. フロー・ソースのリストをレビューし、フロー・ソースを必要に応じて変更します。

   フロー・ソースの構成について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
5. 「フロー・ソース」ウィンドウを閉じます。
6. 「**管理**」タブ・メニューで、「**変更のデプロイ**」をクリックします。

脆弱性評価情報のインポート

脆弱性評価 (VA) 情報をインポートすることにより、アクティブなホスト、オープン・ポート、および潜在的な脆弱性を識別できます。

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、「**データ・ソース**」 > 「**脆弱性**」をクリックします。
3. 「**VA スキャナー**」アイコンをクリックします。
4. ツールバーで、「**追加**」をクリックします。
5. パラメーターの値を入力します。

   パラメーターは、追加するスキャナー・タイプによって異なります。詳しくは、「*脆弱性評価の構成ガイド*」を参照してください。

   重要: CIDR 範囲により、QRadar SIEM がスキャン結果に統合するネットワークが指定されます。例えば、192.168.0.0/16 ネットワークに対してスキャンを行う場合に CIDR 範囲として 192.168.1.0/24 を指定した場合、192.168.1.0/24 範囲からの結果のみが統合されます。
6. 「**保存**」をクリックします。
7. 「**管理**」タブ・メニューで、「**変更のデプロイ**」をクリックします。
8. 「**VA スキャナーのスケジュール**」アイコンをクリックします。
9. 「**追加**」をクリックします。
10. スキャン実行頻度の条件を指定します。

    スキャン・タイプによっては、これには、QRadar SIEM がスキャン結果をインポートする頻度または新規スキャンを開始する頻度が含まれます。また、スキャン結果に含めるポートも指定する必要があります。
11. 「**保存**」をクリックします。

QRadar SIEM のチューニング

環境の要件を満たすように QRadar SIEM をチューニングできます。

QRadar SIEM をチューニングする前に、QRadar SIEM が、ネットワーク上のサーバーの検出、イベントおよびフローの保管、および既存のルールに基づくオフェンスの作成を行えるようにするために、1 日待機します。

管理者は以下のチューニング・タスクを実行できます。

- 「**ログ・アクティビティー**」および「**ネットワーク・アクティビティー**」の「**クイック・フィルター**」プロパティーでペイロード索引を有効にすることにより、イベントおよびフローのペイロード検索を最適化する。
- サーバーを自動または手動でビルディング・ブロックに追加することにより、より迅速な初期デプロイメントおよびより簡単なチューニングを提供する。
- カスタム・ルールおよびアノマリ検出ルールを作成または変更することにより、イベント、フロー、およびオフェンス条件への応答を構成する。

- ネットワーク内の各ホストが、最新のルール、ディスカバー済みのサーバー、およびネットワーク階層に基づくオフェンスを作成することを確認する。

ペイロード索引付け

「**ログ・アクティビティー**」タブおよび「**ネットワーク・アクティビティー**」タブで使用可能な「**クイック・フィルター**」機能を使用して、イベントおよびフローのペイロードを検索します。

「**クイック・フィルター**」を最適化するために、ペイロード索引の「**クイック・フィルター**」プロパティーを有効にできます。

ペイロード索引付けを有効にすることにより、システム・パフォーマンスが低下する可能性があります。「**クイック・フィルター**」プロパティーでペイロード索引付けを有効にした後に、索引統計をモニターしてください。

索引管理および統計について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

ペイロード索引付けの有効化

「**ログ・アクティビティー**」および「**ネットワーク・アクティビティー**」の「**クイック・フィルター**」プロパティーでペイロード索引を有効にすることにより、イベントおよびフローのペイロード検索を最適化できます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・ペインで、「**システム構成**」をクリックします。
3. 「**索引管理**」アイコンをクリックします。
4. 「**クイック検索**」フィールドに、**クイック・フィルター**と入力します。
5. 索引付けする「**クイック・フィルター**」プロパティーをクリックします。
6. 「**索引の有効化**」をクリックします。
7. 「**保存**」をクリックします。
8. 「**OK**」をクリックします。
9. オプション: ペイロード索引を無効にするには、以下のオプションのいずれかを選択します。
   - 「**索引の無効化**」をクリックする。
   - プロパティーを右クリックして、メニューから「**索引の無効化**」を選択する。

次のタスク

「索引管理」ウィンドウに表示されるパラメーターの詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

サーバーおよびビルディング・ブロック

QRadar SIEM では、ネットワーク内のサーバーが自動的にディスカバーおよび分類されるため、初期デプロイメントをより迅速に行うことができ、ネットワークの変更が発生した場合にも簡単にチューニングできます。

サーバー・タイプに対する適切なルールが確実に適用されるようにするため、個別のデバイスまたはデバイスのアドレス範囲全体を追加することができます。固有のプロトコルに適合しないサーバー・タイプを、該当するホスト定義ビルディング・ブロックに手動で入力できます。例えば、以下のサーバー・タイプをビルディング・ブロックに追加することにより、追加のフォールス・ポジティブ・チューニングを行う必要がなくなります。

- ネットワーク管理サーバーを「**BB:HostDefinition: Network Management Servers**」ビルディング・ブロックに追加する。
- プロキシー・サーバーを「**BB:HostDefinition: Proxy Servers**」ビルディング・ブロックに追加する。
- ウィルスおよび Windows アップデート・サーバーを「**BB:HostDefinition: Virus Definition and Other Update Servers**」ビルディング・ブロックに追加する。
- VA スキャナーを「**BB-HostDefinition: VA Scanner Source IP**」ビルディング・ブロックに追加する。

サーバー・ディスカバリー機能では、アセット・プロファイル・データベースを使用して、ネットワーク上の複数タイプのサーバーをディスカバーします。サーバー・ディスカバリーにより自動的にディスカバーされたサーバーがリストされ、ビルディング・ブロックに含めるサーバーを選択できます。

サーバーのディスカバーについて詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

ビルディング・ブロックを使用して、特定のルール・テストを別のルールで再利用することができます。ビルディング・ブロックを使用して QRadar SIEM をチューニングし、追加の相関ルールを有効にすることにより、フォールス・ポジティブの数を削減することができます。

ビルディング・ブロックへの自動でのサーバーの追加

ビルディング・ブロックにサーバーを自動的に追加できます。

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・ペインで、「**サーバー・ディスカバリー**」をクリックします。
3. 「**サーバー・タイプ**」リストで、ディスカバーするサーバー・タイプを選択します。

   残りのパラメーターはデフォルトのままにします。
4. 「**サーバーのディスカバー**」をクリックします。
5. 「一致するサーバー」ペインで、サーバー・ロールに割り当てるすべてのサーバーのチェック・ボックスを選択します。
6. 「**選択したサーバーの承認**」をクリックします。

   要確認: IP アドレスまたはホスト名を右クリックして、DNS 解決情報を表示できます。

ビルディング・ブロックへの手動でのサーバーの追加

サーバーが自動検出されない場合、そのサーバーを対応するホスト定義ビルディング・ブロックに手動で追加できます。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・ペインで、「**ルール**」をクリックします。
3. 「**表示**」リストで、「**ビルディング・ブロック**」を選択します。
4. 「**グループ**」リストで、「**ホスト定義**」を選択します。

   ビルディング・ブロックの名前はサーバー・タイプに対応しています。例えば、「**BB:HostDefinition: Proxy Servers**」は環境内のすべてのプロキシー・サーバーに適用されます。
5. ホストまたはネットワークを手動で追加するには、環境に適した対応するホスト定義ビルディング・ブロックをダブルクリックします。
6. 「**ビルディング・ブロック**」フィールドで、「**送信元または宛先 IP のいずれかが次のいずれかの場合 (when either the source or destination IP is one of the following)**」の後の下線が付いた値をクリックします。
7. 「**IP アドレスまたは CIDR の入力 (Enter an IP address or CIDR)**」フィールドに、ビルディング・ブロックに割り当てるホスト名または IP アドレス範囲を入力します。
8. 「**追加**」をクリックします。
9. 「**送信**」をクリックします。
10. 「**終了**」をクリックします。
11. 追加するサーバー・タイプごとにこれらの手順を繰り返します。

ルールの構成

「**ログ・アクティビティー**」、「**ネットワーク・アクティビティー**」、および「**オフェンス**」の各タブから、ルールまたはビルディング・ブロックを構成できます。

手順

1. 「**オフェンス**」タブをクリックします。
2. 調査するオフェンスをダブルクリックします。
3. 「**表示**」 > 「**ルール**」をクリックします。
4. ルールをダブルクリックします。

   ルールをさらにチューニングできます。ルールのチューニングについて詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
5. ルール・ウィザードを閉じます。
6. 「ルール」ページで、「**アクション**」をクリックします。
7. オプション: オフェンスの保存期間の経過後にオフェンスがデータベースから削除されないようにする場合は、「**オフェンスの保護**」を選択します。
8. オプション: オフェンスを QRadar SIEM ユーザーに割り当てる場合は、「**割り当て**」を選択します。

関連概念:

4 ページの『QRadar SIEM のルール』
ルールは、イベント、フロー、またはオフェンスに対してテストを実行し、すべてのテスト条件が満たされた場合に応答を生成します。

SIM モデルのクリーンアップ

SIEM モデルをクリーンアップして、各ホストが、確実に最新のルール、ディスカバー済みのサーバー、およびネットワーク階層に基づくオフェンスを作成するようにします。

手順

1. 「**管理**」タブをクリックします。
2. ツールバーで、「**拡張**」 > 「**SIM モデルのクリーンアップ**」を選択します。
3. 以下の必須指定のオプションをクリックします。

   「ソフト・クリーン」はオフェンスを非アクティブに設定します。

   「ソフト・クリーン」をオプションの「すべてのオフェンスを非アクティブにする」とともに使用するとすべてのオフェンスがクローズされます。

   「ハード・クリーン」はすべてのエントリーを削除します。
4. 「**データ・モデルをリセットしますか?**」をクリックします。
5. 「**次へ進む**」をクリックします。
6. SIM リセット処理が完了したら、ブラウザーを最新表示します。

タスクの結果

SIM モデルをクリーンアップすると、既存のオフェンスはすべてクローズされます。SIM モデルのクリーンアップは、既存のイベントおよびフローには影響しません。

第 3 章 QRadar SIEM の使用開始

IBM Security QRadar SIEM を使用を開始するために、イベント、フロー、およびアセットの検索について説明します。また、オフェンスを調査してレポートを作成する方法についても説明します。

例えば、情報を検索するために、「**ログ・アクティビティー**」タブおよび「**ネットワーク・アクティビティー**」タブ内のデフォルトの保存済み検索を使用できます。独自のカスタム検索を作成して保存することもできます。

管理者は以下の作業を実行できます。

- 特定の条件を使用してイベント・データを検索し、検索条件に一致するイベントを結果リストに表示する。イベント・データの列を選択、編成、およびグループ化する。
- フロー・データをリアルタイムで視覚的にモニターおよび調査する。または、表示されるフローをフィルタリングするための拡張検索を実行する。フロー情報を表示して、ネットワーク・トラフィックの通信方法および通信内容を判別する。
- 学習済みのアセットをすべて表示する、または環境内の特定のアセットを検索する。
- オフェンス、送信元および宛先 IP アドレス、ネットワーク振る舞い、およびネットワーク上のアノマリを調査する。
- デフォルト・レポートまたはカスタム・レポートを編集、作成、スケジュール、および配布する。

イベントの検索

QRadar SIEM が過去 6 時間に受信したすべての認証イベントを検索できます。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. ツールバーで、「**検索**」 > 「**新規検索**」を選択します。
3. 「時刻範囲」ペインで、イベント検索の時刻範囲を定義します。
   a. 「**最新**」をクリックします。
   b. 「**最新**」リストで、「**過去 6 時間**」を選択します。
4. 「検索パラメーター」ペインで、以下のように検索パラメーターを定義します。
   a. 最初のリストで、「**カテゴリー**」を選択します。
   b. 2 番目のリストで、「**次と等しい**」を選択します。
   c. 「**上位カテゴリー**」リストで、「**認証**」を選択します。
   d. 「**下位カテゴリー**」リストで、デフォルト値の「**すべて**」を受け入れます。
   e. 「**フィルターの追加**」をクリックします。
5. 「列定義」ペインで、「**表示**」リストの「**イベント名**」を選択します。
6. 「**検索**」をクリックします。

イベント検索条件の保存

指定のイベント検索条件を後で使用するために保存できます。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. ツールバーで、「**条件の保存**」をクリックします。
3. 「**検索名**」フィールドに、**Example Search 1** と入力します。
4. 「タイム・スパン・オプション」ペインで、「**最新**」をクリックします。
5. 「**最新**」リストで、「**過去 6 時間**」を選択します。
6. 「**クイック検索に含める**」をクリックします。
7. 「**ダッシュボードに含める**」をクリックします。

   「**ダッシュボードに含める**」が表示されていない場合、「**検索**」 > 「**検索の編集**」をクリックして、「列定義」ペインで「**イベント名**」を選択していることを確認します。
8. 「**OK**」をクリックします。

次のタスク

時系列グラフを構成します。詳しくは、『時系列グラフの構成』を参照してください。

時系列グラフの構成

特定の時間間隔検索により突き合わされたレコードを表す対話式時系列グラフを表示できます。

手順

1. グラフのタイトル・バーで、「**構成**」アイコンをクリックします。
2. 「**グラフの値**」リストで、「**宛先 IP (固有の数)**」を選択します。
3. 「**グラフ・タイプ**」リストで、「**時系列**」を選択します。
4. 「**時系列データのキャプチャー**」をクリックします。
5. 「**保存**」をクリックします。
6. 「**詳細の更新**」をクリックします。
7. 検索結果をフィルタリングします。
   a. フィルタリングするイベントを右クリックします。
   b. 「**イベント名が <イベント名> でのフィルター**」をクリックします。
8. ユーザー名ごとにグループ化されたイベント・リストを表示するために、「**表示**」リストから「**ユーザー名**」を選択します。
9. 検索が「**ダッシュボード**」タブに表示されていることを確認します。
   a. 「**ダッシュボード**」タブをクリックします。
   b. 「**新規ダッシュボード**」アイコンをクリックします。
   c. 「**名前**」フィールドに、**Example Custom Dashboard** と入力します。
   d. 「**OK**」をクリックします。

e. 「**項目の追加**」リストで、「**ログ・アクティビティー**」 > 「**イベント検索**」 > 「**Example Search 1**」を選択します。

タスクの結果

保存済みイベント検索の結果がダッシュボードに表示されます。

フローの検索

フロー・データをリアルタイムで検索、モニター、および調査できます。

拡張検索を実行して、表示されるフローをフィルタリングすることもできます。フロー情報を表示して、ネットワーク・トラフィックの通信方法および通信内容を判別します。

手順

1. 「**ネットワーク・アクティビティー**」タブをクリックします。
2. ツールバーで、「**検索**」 > 「**新規検索**」をクリックします。
3. 「時刻範囲」ペインで、以下のようにしてフロー検索の時刻範囲を定義します。
   a. 「**最新**」をクリックします。
   b. 「**最新**」リストで、「**過去 6 時間**」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. 最初のリストで、「**フローの向き**」を選択します。
   b. 2 番目のリストで、「**次と等しい**」を選択します。
   c. 3 番目のリストで、「**R2L**」を選択します。
   d. 「**フィルターの追加**」をクリックします。
5. 「列定義」ペインの「**表示**」リストで、「**アプリケーション**」を選択します。
6. 「**検索**」をクリックします。

タスクの結果

過去 6 時間の、フローの向きがリモートからローカル (R2L) のすべてのフローが表示され、「**アプリケーション名**」フィールドでソートされます。

フロー検索条件の保存

指定のフロー検索条件を後で使用するために保存できます。

手順

1. 「**ネットワーク・アクティビティー**」タブのツールバーで、「**条件の保存**」をクリックします。
2. 「**検索名**」フィールドに、名前 **Example Search 2** を入力します。
3. 「**最新**」リストで、「**過去 6 時間**」を選択します。
4. 「**ダッシュボードに含める**」および「**クイック検索に含める**」をクリックします。
5. 「**OK**」をクリックします。

次のタスク

ダッシュボード項目を作成します。詳しくは、『ダッシュボード項目の作成』を参照してください。

ダッシュボード項目の作成

保存済みフロー検索条件を使用してダッシュボード項目を作成できます。

手順

1. 「**ネットワーク・アクティビティー**」ツールバーで、「**クイック検索**」 > 「**Example Search 2**」を選択します。
2. 検索がダッシュボードに含まれていることを確認します。
   a. 「**ダッシュボード**」タブをクリックします。
   b. 「**ダッシュボードの表示**」リストで、「**Example Custom Dashboard**」を選択します。
   c. 「**項目の追加**」リストで、「**フロー検索**」 > 「**Example Search 2**」を選択します。
3. ダッシュボード・グラフを構成します。
   a. 「**設定**」アイコンをクリックします。
   b. 構成オプションを使用して、グラフ化する値、表示するオブジェクトの数、グラフ・タイプ、またはグラフ内に表示する時刻範囲を変更します。
4. グラフに現在表示されているフローを調査するには、「**ネットワーク・アクティビティーで表示**」をクリックします。

タスクの結果

「ネットワーク・アクティビティー」ページに、時系列グラフのパラメーターに一致する結果が表示されます。時系列グラフについて詳しくは、「*IBM Security QRadar SIEM ユーザーズ・ガイド*」を参照してください。

アセットの検索

「**アセット**」タブにアクセスすると、ネットワーク内でディスカバーされたすべてのアセットが取り込まれた「アセット」ページが表示されます。このリストを絞り込むために、検索パラメーターを構成して調査するアセット・プロファイルのみを表示することができます。

このタスクについて

検索機能を使用して、ホスト・プロファイル、アセット、およびアイデンティティー情報を検索します。アイデンティティー情報は、ネットワーク上の DNS 情報、ユーザー・ログイン、MAC アドレスなどの詳細を提供します。

例えば、以下のとおりです。

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・ペインで、「**アセット・プロファイル**」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. 保存済み検索をロードする場合は、以下の手順を実行します。
   a. オプション: 「**グループ**」リストで、「**使用可能な保存済み検索**」リストに表示するアセット検索グループを選択します。
   b. 次のオプションのいずれかを選択してください。
      - 「**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**」リストで、ロードする保存済み検索を選択します。
   c. 「**ロード**」をクリックします。
5. 「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. 最初のリストで、検索対象のアセット・パラメーターを選択します。例えば、「**ホスト名**」、「**脆弱性リスク分類**」、「**テクニカル・オーナー**」です。
   b. 2 番目のリストで、検索に使用する修飾子を選択します。
   c. 「**項目**」フィールドに、検索パラメーター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これらのステップを繰り返します。
6. 「**検索**」をクリックします。

例

CVE ID: CVE-2010-000 がアクティブにエクスプロイトされているという通知を受け取りました。デプロイメント内のホストがこのエクスプロイトに対して脆弱かどうかを判別するために、以下の手順を実行します。

1. 検索パラメーターのリストから、「**脆弱性外部リファレンス**」を選択します。
2. 「**CVE**」を選択します。
3. 2010-000 と入力し、この特定の CVE ID に対して脆弱なすべてのホストのリストを表示します。

詳しくは、Open Source Vulnerability Database Web サイト (*http://osvdb.org/*) および National Vulnerability Database (*http://nvd.nist.gov/*) を参照してください。

オフェンス調査

「**オフェンス**」タブを使用して、オフェンス、送信元および宛先 IP アドレス、ネットワーク振る舞い、およびネットワーク上のアノマリを調査できます。

QRadar SIEM は、複数のネットワークにまたがって存在する宛先 IP アドレスを持つイベントおよびフローを同一オフェンス内で相関付けし、最終的には同じネット

ワーク・インシデントに相関付けることができます。これにより、ネットワーク内の各オフェンスを効率良く調査することができます。

オフェンスの表示

ネットワーク内の各オフェンスを調査できます。

例えば、オフェンス、送信元および宛先 IP アドレス、ネットワーク振る舞い、およびネットワーク上のアノマリを調査できます。

手順

1. 「**オフェンス**」タブをクリックします。
2. 調査するオフェンスをダブルクリックします。
3. ツールバーで、「**表示**」 > 「**宛先**」を選択します。

   各宛先を調査して、宛先が危険にさらされていたり、疑わしい振る舞いを示したりしていないかどうかを判別できます。
4. ツールバーで、「**イベント**」をクリックします。

タスクの結果

「イベントのリスト」ウィンドウに、オフェンスに関連付けられているすべてのイベントが表示されます。イベントを検索、ソート、およびフィルタリングできます。

例: PCI レポート・テンプレートの有効化

「**レポート**」タブを使用して、レポート・テンプレートの有効化、無効化、および編集を行えます。

この入門タスクでは、Payment Card Industry (PCI) レポート・テンプレートを有効にします。

手順

1. 「**レポート**」タブをクリックします。
2. 「**非アクティブ・レポートの非表示**」チェック・ボックスをクリアします。
3. 「**グループ**」リストで、「**コンプライアンス**」 > 「**PCI**」を選択します。
4. 以下のようにして、リスト上のすべてのレポート・テンプレートを選択します。
   a. リスト上の最初のレポートをクリックします。
   b. シフト・キーを押したままにしてリスト上の最後のレポートをクリックすることにより、すべてのレポート・テンプレートを選択します。
5. 「**アクション**」リストで、「**スケジューリングの切り替え**」を選択します。
6. 生成されたレポートにアクセスします。
   a. 「**生成済みレポート**」列のリストから、表示するレポートのタイム・スタンプを選択します。
   b. 「**フォーマット**」列で、表示するレポート・フォーマットのアイコンをクリックします。

例: 保存済み検索に基づくカスタム・レポートの作成

検索をインポートするかまたはカスタム条件を作成することにより、レポートを作成できます。

このタスクについて

この入門タスクでは、 17 ページの『イベントの検索』で作成したイベントおよびフローの検索に基づくレポートを作成します。

手順

1. 「**レポート**」タブをクリックします。
2. 「**アクション**」リストで、「**作成**」を選択します。
3. 「**次へ**」をクリックします。
4. レポート・スケジュールを構成します。
   a. 「**毎日**」オプションを選択します。
   b. 「**月曜日**」、「**火曜日**」、「**水曜日**」、「**木曜日**」、および「**金曜日**」の各オプションを選択します。
   c. リストを使用して、「**8:00**」および「**AM**」を選択します。
   d. 「**はい - レポートを手動で生成します**」オプションが選択されていることを確認します。
   e. 「**次へ**」をクリックします。
5. レポート・レイアウトを構成します。
   a. 「**方向**」リストで、「**横長**」を選択します。
   b. 2 つのグラフ・コンテナーがあるレイアウトを選択します。
   c. 「**次へ**」をクリックします。
6. 「**レポート・タイトル**」フィールドに、**Sample Report** と入力します。
7. 上部のグラフ・コンテナーを構成します。
   a. 「**グラフ・タイプ**」リストで、「**イベント/ログ**」を選択します。
   b. 「**グラフ・タイトル**」フィールドに、**Sample Event Search** と入力します。
   c. 「**イベント/ログの限定数: 上位**」リストで、「**10**」を選択します。
   d. 「**グラフ・タイプ**」リストで、「**積み重ね棒**」を選択します。
   e. 「**直近 1 日 (24 時間) の全データ**」をクリックします。
   f. 「**このイベント・レポートは次に基づく**」リストで、「**Example Search 1**」を選択します。

      残りのパラメーターは、「Example Search 1」保存済み検索の設定を使用して自動的に取り込まれます。
   g. 「**コンテナー詳細の保存**」をクリックします。
8. 下部のグラフ・コンテナーを構成します。
   a. 「**グラフ・タイプ**」リストで、「**フロー**」を選択します。
   b. 「**グラフ・タイトル**」フィールドに、**Sample Flow Search** と入力します。
   c. 「**フローの限定数: 上位**」リストで、「**10**」を選択します。
   d. 「**グラフ・タイプ**」リストで、「**積み重ね棒**」を選択します。

e. 「**直近 1 日 (24 時間) の全データ**」をクリックします。

f. 「**使用可能な保存済み検索**」リストで、「**Example Search 2**」を選択します。

残りのパラメーターは、「Example Search 2」保存済み検索の設定を使用して自動的に取り込まれます。

g. 「**コンテナー詳細の保存**」をクリックします。

9. 「**次へ**」をクリックします。
10. 「**次へ**」をクリックします。
11. レポート・フォーマットを選択します。
    a. 「**PDF**」と「**HTML**」のチェック・ボックスを選択します。
    b. 「**次へ**」をクリックします。
12. レポート配布チャネルを選択します。
    a. 「**レポート・コンソール**」をクリックします。
    b. 「**E メール**」をクリックします。
    c. 「**レポートの宛先 E メール・アドレスの入力 (複数可)**」フィールドに、E メール・アドレスを入力します。
    d. 「**レポートを添付ファイルとして含める**」をクリックします。
    e. 「**次へ**」をクリックします。
13. 最後のレポート・ウィザード詳細を完了します。
    a. 「**レポートの説明**」フィールドに、テンプレートの説明を入力します。
    b. 「**はい - ウィザードが完了したらこのレポートを実行**」をクリックします。
    c. 「**終了**」をクリックします。
14. 「**生成済みレポート**」列のリスト・ボックスを使用して、レポートのタイム・スタンプを選択します。

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。

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。

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。

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

この用語集は、IBM Security QRadar SIEM ソフトウェアおよび製品の用語と定義を示します。

次の相互参照がこの用語集で使用されています。

- ...を参照 は、非優先用語から優先用語を参照するか、省略語から省略しない形式を参照します。
- ...も参照 は、関連する用語または対になる用語を参照します。

その他の用語および定義については、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』 『B』 『C』 30 ページの『D』 30 ページの『E』 31 ページの『F』 31 ページの『G』 31 ページの『H』 31 ページの『I』 32 ページの『L』 33 ページの『M』 33 ページの『N』 33 ページの『O』 34 ページの『P』 34 ページの『Q』 34 ページの『R』 35 ページの『S』 35 ページの『T』 36 ページの『V』 36 ページの『W』

A

アキュムレーター (accumulator)
演算の 1 つのオペランドを格納できるレジスター。後でその演算の結果で置換される。

アクティブ・システム (active system)
高可用性 (HA) クラスターで、サービスがすべて実行されているシステム。

アドレス解決プロトコル (ARP) (Address Resolution Protocol (ARP))
ローカル・エリア・ネットワークで IP アドレスをネットワーク・アダプター・アドレスに動的にマップするプロトコル。

管理共有 (administrative share)
管理特権のないユーザーに非表示になっているネットワーク・リソース。管理共有により、管理者はネットワーク・システム上のすべてのリソースにアクセスできる。

アノマリ (anomaly)
予期されるネットワークの振る舞いからの逸脱。

アプリケーション・シグネチャー (application signature)
パケット・ペイロードを調べることによって導き出される特性の固有のセット。特定のアプリケーションを識別するために使用される。

ARP アドレス解決プロトコル (Address Resolution Protocol) を参照。

ARP リダイレクト (ARP Redirect)
ネットワークに問題が存在する場合にホストに通知する ARP 方法。

ASN 自律システム番号 (autonomous system number) を参照。

アセット (asset)
稼働環境にデプロイされている、またはデプロイされる予定の管理可能なオブジェクト。

自律システム番号 (ASN) (autonomous system number (ASN))
TCP/IP で、IP アドレスを割り当てるのと同じ中央の認証局によって自律システムに割り当てられる番号。自律システム番号により、自律システムを識別するルーティング・アルゴリズムを自動化できる。

B

振る舞い (behavior)
演算またはイベントの観測可能な影響。その結果を含む。

C

CIDR クラスレス・ドメイン間ルーティング (Classless Inter-Domain Routing) を参照。

クラスレス・ドメイン間ルーティング (CIDR) (Classless Inter-Domain Routing (CIDR))
クラス C のインターネット・プロトコル

(IP) アドレスを追加する方法。アドレスは、インターネット・サービス・プロバイダー (ISP) の顧客が使用するために、そのプロバイダーに与えられる。CIDR アドレスは、ルーティング・テーブルのサイズを削減し、組織内でより多くの IP アドレスを使用可能にする。

クライアント (client)
サーバーからのサービスを要求するソフトウェア・プログラムまたはコンピューター。

クラスター仮想 IP アドレス (cluster virtual IP address)
プライマリー・ホストまたはセカンダリー・ホストと、HA クラスターとの間で共有される IP アドレス。

統合間隔 (coalescing interval)
イベントがバンドルされる間隔。イベントのバンドル化は、10 秒間隔で発生する。現在統合中のイベントと一致しない最初のイベントから開始される。統合間隔内に、最初に一致する 3 つのイベントがバンドル化され、イベント・プロセッサーに送信される。

共通脆弱性評価システム (CVSS) (Common Vulnerability Scoring System (CVSS))
脆弱性の重大度を測定する評価システム。

コンソール (console)
オペレーターがシステム操作を制御し監視できるディスプレイ装置。

コンテンツ・キャプチャー (content capture)
構成可能なペイロードの量をキャプチャーし、そのデータをフロー・ログに格納するプロセス。

資格情報 (credential)
ユーザーまたはプロセスに特定のアクセス権限を付与する情報のセット。

信頼性 (credibility)
イベントまたはオフェンスの整合性を判別するために使用される 0 から 10 までの数値による評価。信頼性は、複数のソースが同じイベントまたはオフェンスを報告すると上がる。

CVSS 共通脆弱性評価システム (Common Vulnerability Scoring System) を参照。

D

データベース・リーフ・オブジェクト (database leaf object)
データベース階層の終端のオブジェクトまたはノード。

データ・ポイント (datapoint)
ある時点でのメトリックの計算値。

デバイス・サポート・モジュール (DSM) (Device Support Module (DSM))
複数のログ・ソースから受信したイベントを解析し、出力として表示できる標準の分類形式にそれらを変換する構成ファイル。

DHCP 動的ホスト構成プロトコル (Dynamic Host Configuration Protocol) を参照。

DNS ドメイン・ネーム・システム (Domain Name System) を参照。

ドメイン・ネーム・システム (DNS) (Domain Name System (DNS))
ドメイン・ネームを IP アドレスにマップする分散データベース・システム。

DSM デバイス・サポート・モジュール (Device Support Module) を参照。

重複フロー (duplicate flow)
異なるフロー・ソースから受信した同じデータ伝送の複数インスタンス。

動的ホスト構成プロトコル (DHCP) (Dynamic Host Configuration Protocol (DHCP))
中央で構成情報を管理するために使用される通信プロトコル。例えば、DHCP はネットワーク内のコンピューターに IP アドレスを自動的に割り当てる。

E

暗号化 (encryption)
コンピューター・セキュリティーで、元のデータを入手できないようにするか、暗号化解除プロセスの使用によってのみ入手できるようにすることで、判読不能な形式にデータを変換するプロセス。

エンドポイント (endpoint)
環境内の API またはサービスのアドレ

ス。API は、エンドポイントを公開し、同時に他のサービスのエンドポイントを呼び出す。

外部スキャン・アプライアンス (external scanning appliance)
ネットワーク内のアセットに関する脆弱性情報を収集するためにネットワークに接続されているマシン。

F

フォールス・ポジティブ (false positive)
ポジティブ (サイトが攻撃に対して脆弱であることを示す) であると分類されたが、実際にはネガティブ (脆弱ではない) とユーザーが判断するテスト結果。

フロー (flow)
対話時にリンク経由で通過するデータの単一の伝送。

フロー・ログ (flow log)
フロー・レコードの集合。

フロー・ソース (flow sources)
フローのキャプチャー元。フロー・ソースは、フローが管理対象ホストにインストールされているハードウェアから発生するときには内部として分類され、フローがフロー・コレクターに送信されるときには外部として分類される。

転送先 (forwarding destination)
未加工のデータと正規化されたデータをログ・ソースとフロー・ソースから受信する 1 つ以上のベンダー・システム。

FQDN 完全修飾ドメイン名 (fully qualified domain name) を参照。

FQNN 完全修飾ネットワーク名 (fully qualified network name) を参照。

完全修飾ドメイン名 (FQDN) (fully qualified domain name (FQDN))
インターネット通信で、ドメイン名のサブネームをすべて含むホスト・システムの名前。完全修飾ドメイン名の例として、rchland.vnet.ibm.com がある。

完全修飾ネットワーク名 (FQNN) (fully qualified network name (FQNN))
ネットワーク階層で、すべての部門を含むオブジェクトの名前。完全修飾ネットワーク名の例として、CompanyA.Department.Marketing がある。

G

ゲートウェイ (gateway)
異なるネットワーク・アーキテクチャーのネットワークまたはシステムを接続するために使用されるデバイスまたはプログラム。

H

HA 高可用性 (high availability) を参照。

HA クラスター (HA cluster)
1 台のプライマリー・サーバーおよび 1 台のセカンダリー・サーバーで構成される高可用性構成。

ハッシュ・ベースのメッセージ認証コード (HMAC) (Hash-Based Message Authentication Code (HMAC))
暗号ハッシュ機能と秘密鍵を使用する暗号コード。

高可用性 (HA) (high availability (HA))
ノードまたはデーモンの障害が発生したときにワークロードをクラスター内の残りのノードに再分散できるクラスター化されたシステム関連。

HMAC
ハッシュ・ベースのメッセージ認証コード (Hash-Based Message Authentication Code) を参照。

ホスト・コンテキスト (host context)
コンポーネントをモニターして、各コンポーネントが予期されているとおりに動作していることを確認するサービス。

I

ICMP Internet Control Message Protocol を参照。

アイデンティティー (identity)
個人、組織、または項目を表すデータ・ソースの属性の集合。

IDS 侵入検知システム (intrusion detection system) を参照。

Internet Control Message Protocol (ICMP)
データグラム内のエラーを報告する目的などで、ソース・ホストと通信するためにゲートウェイが使用するインターネット・プロトコル。

インターネット・プロトコル (IP) (Internet Protocol (IP))
ネットワークまたは相互接続ネットワーク経由でデータをルーティングするプロトコル。このプロトコルは、上位のプロトコル層と物理ネットワークとの間の仲介として機能する。伝送制御プロトコル (Transmission Control Protocol) も参照。

インターネット・サービス・プロバイダー (ISP) (Internet service provider (ISP))
インターネットへのアクセスを提供する組織。

侵入検知システム (IDS) (intrusion detection system (IDS))
ネットワークまたはホスト・システムの一部であるモニター対象リソースに対する攻撃の試行や遂行を検出するソフトウェア。

侵入防止システム (IPS) (intrusion prevention system (IPS))
不正の可能性があるアクティビティーを拒否しようとするシステム。拒否のメカニズムには、フィルター処理、トラッキング、速度制限の設定などが考えられる。

IP インターネット・プロトコル (Internet Protocol) を参照。

IP マルチキャスト (IP multicast)
単一のマルチキャスト・グループを形成するシステムの 1 セットへのインターネット・プロトコル (IP) データグラムの伝送。

IPS 侵入防止システム (intrusion prevention system) を参照。

ISP インターネット・サービス・プロバイダー (Internet service provider) を参照。

K

鍵ファイル (key file)
コンピューター・セキュリティーにおいて、公開鍵、秘密鍵、トラステッド・ルート、および証明書を含むファイル。

L

L2L ローカルからローカル (Local To Local) を参照。

L2R ローカルからリモート (Local To Remote) を参照。

LAN ローカル・エリア・ネットワーク (Local Area Network) を参照してください。

LDAP Lightweight Directory Access Protocol を参照。

リーフ (leaf)
ツリーで、子を持たないエントリーまたはノード。

Lightweight Directory Access Protocol (LDAP)
TCP/IP を使用して X.500 モデルをサポートするディレクトリーへのアクセスを提供するオープン・プロトコル。より複雑な X.500 ディレクトリー・アクセス・プロトコル (DAP) のリソース要件は必要とされない。例えば、インターネット・ディレクトリーまたはイントラネット・ディレクトリー内のユーザー、組織、その他のリソースを見つけるために LDAP を使用できる。

ライブ・スキャン (live scan)
セッション名に基づいてスキャン結果からレポート・データを生成する脆弱性スキャン。

ローカル・エリア・ネットワーク (LAN) (local area network (LAN))
制限された領域内 (単一のビルやキャンパスなど) の複数のデバイスを接続するネットワーク。より大規模なネットワークに接続することもできる。

ローカルからローカル (L2L) (Local To Local (L2L)) あるローカル・ネットワークから別のローカル・ネットワークへの内部トラフィック関連。

ローカルからリモート (L2R) (Local To Remote (L2R)) あるローカル・ネットワークから別のリモート・ネットワークへの内部トラフィック関連。

ログ・ソース (log source)
イベント・ログの発生元のセキュリティー装置またはネットワーク装置。

ログ・ソース拡張 (log source extension)
イベント・ペイロードからのイベントを識別し分類するために必要な正規表現パターンをすべて格納している XML ファイル。

M

判定機能 (magistrate)
定義されているカスタム・ルールに照らし合わせてネットワーク・トラフィックおよびセキュリティー・イベントを分析する内部コンポーネント。

マグニチュード (magnitude)
特定のオフェンスの相対的な重要性の尺度。マグニチュードは、関連性、重大度、および信頼性から計算される重みづけされた値である。

N

NAT ネットワーク・アドレス変換 (Network Address Translation) を参照。

NetFlow
ネットワーク・トラフィックのフロー・データをモニターする Cisco のネットワーク・プロトコル。 NetFlow データには、クライアントおよびサーバーの情報、使用するポート、およびネットワークに接続されているスイッチとルーターを流れるバイト数とパケット数が含まれる。データは、データ分析が行われる NetFlow コレクターに送信される。

ネットワーク・アドレス変換 (NAT) (Network Address Translation (NAT))
ファイアウォールでの、安全なインターネット・プロトコル (IP) アドレスから外部の登録アドレスへの変換。これにより、外部ネットワークとの通信が可能になるが、ファイアウォール内で使用される IP アドレスはマスクされる。

ネットワーク階層 (network hierarchy)
ネットワーク・オブジェクトの階層型コレクションであるコンテナーの一種。

ネットワーク層 (network layer)
OSI アーキテクチャーで、予測可能なサービス品質を持つオープン・システム間にパスを確立するサービスを提供する層。

ネットワーク・オブジェクト (network object)
ネットワーク階層のコンポーネント。

ネットワークの重み (network weight)
各ネットワークに適用される、ネットワークの重要性を示す数値。ネットワークの重みは、ユーザーによって定義される。

O

オフェンス (offense)
モニターされた状態に対応して送信されるメッセージまたは生成されるイベント。例えば、オフェンスは、ポリシー違反があったかどうか、ネットワークが攻撃されているかどうかなどに関する情報を提供する。

オフサイト・ソース (offsite source)
正規化されたデータをイベント・コレクターに転送する、プライマリー・サイトから離れた場所に存在するデバイス。

オフサイト・ターゲット (offsite target)
イベント・コレクターからイベント・フローまたはデータ・フローを受信する、プライマリー・サイトから離れた場所に存在するデバイス。

オープン・ソース脆弱性データベース (OSVDB) (Open Source Vulnerability Database (OSVDB))
ネットワーク・セキュリティー・コミュニティーがネットワーク・セキュリティー・コミュニティーのために作成した、ネットワーク・セキュリティーの脆弱性に関する技術情報を提供するオープン・ソース・データベース。

オープン・システム間相互接続 (OSI) (open systems interconnection (OSI))
国際標準化機構 (ISO) の規格に沿った、情報交換のためのオープン・システムの相互接続。

OSI オープン・システム間相互接続 (open systems interconnection) を参照。

OSVDB
オープン・ソース脆弱性データベース (Open Source Vulnerability Database) を参照。

P

解析順序 (parsing order)
共通の IP アドレスまたはホスト名を共有するログ・ソースに対して、ユーザーが重要度の順序を定義できるログ・ソース定義。

ペイロード・データ (payload data)
IP フローに含まれるアプリケーション・データ。ヘッダーと管理情報を除く。

プライマリー HA ホスト (primary HA host)
HA クラスターに接続されるメイン・コンピューター。

プロトコル (protocol)
通信ネットワーク内の 2 つ以上のデバイスまたはシステムの間でのデータの通信と転送を制御するルールのセット。

Q

QID マップ (QID Map)
各固有イベントを識別し、そのイベントを下位カテゴリーと上位カテゴリーにマップして、イベントの相関方法と編成方法を決定する分類法。

R

R2L リモートからローカル (Remote To Local) を参照。

R2R リモートからリモート (Remote To Remote) を参照。

recon スキャン行為 (reconnaissance) を参照。

スキャン行為 (reconnaissance (recon))
ネットワーク・リソースの ID に関連する情報を収集する方式。ネットワーク・スキャンやその他の技法を使用してネットワーク・リソース・イベントのリストがコンパイルされ、それらに重大度レベルが割り当てられる。

リファレンス・マップ (reference map)
キーから値への直接マッピング (例えば、ユーザー名からグローバル ID) のデータ・レコード。

マップのリファレンス・マップ (reference map of maps) 2 つのキーが多数の値にマップされたデータ・レコード。例えば、アプリケーションの合計バイト数から送信元 IP へのマッピング。

セットのリファレンス・マップ (reference map of sets) 1 つのキーが多数の値にマップされたデータ・レコード。例えば、特権ユーザーのリストからホストへのマッピング。

リファレンス・セット (reference set)
ネットワーク上のイベントまたはフローから派生した単一エレメントのリスト。例えば、IP アドレスのリストやユーザー名のリスト。

リファレンス・テーブル (reference table)
データ・レコードにより、タイプが割り当てられたキーを他のキーにマップするテーブル。マップ先のキーは単一値にマップされる。

最新表示タイマー (refresh timer)
一定間隔で、手動または自動でトリガーされる内部デバイス。現在のネットワーク・アクティビティー・データを更新する。

関連性 (relevance)
ネットワーク上のイベント、カテゴリー、またはオフェンスの相対的な影響の尺度。

リモートからローカル (R2L) (Remote To Local (R2L)) リモート・ネットワークからローカル・ネットワークへの外部トラフィック。

リモートからリモート (R2R) (Remote To Remote (R2R)) あるリモート・ネットワークから別のリモート・ネットワークへの外部トラフィック。

レポート (report)
照会管理で、照会を実行し、その結果に形式を適用することで生成される書式設定されたデータ。

レポート間隔 (report interval)
構成可能な時間間隔。この間隔の終わりに、イベント・プロセッサーは、取得したすべてのイベント・データとフロー・データをコンソールに送信する必要がある。

ルーティング・ルール (routing rule)
イベント・データがその基準を満たしたときに、条件の集合とその結果として発生するルーティングが実行される条件。

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

スキャナー (scanner)
Web アプリケーション内でソフトウェアの脆弱性を検索する、自動化されたセキュリティー・プログラム。

セカンダリー HA ホスト (secondary HA host)
HA クラスターに接続されているスタンバイ・コンピューター。セカンダリー HA ホストは、プライマリー HA ホストで障害が発生した場合にプライマリー HA ホストの処理を引き継ぐ。

重大度 (severity)
送信元が宛先に及ぼす相対的な脅威の尺度。

Simple Network Management Protocol (SNMP)
複合ネットワーク内のシステムとデバイスをモニターするための一連のプロトコル。管理対象デバイスに関する情報は、管理情報ベース (MIB) に定義され、格納される。

SNMP Simple Network Management Protocol を参照。

SOAP 非集中型分散環境で情報を交換するための、軽量の XML ベース・プロトコル。SOAP は、インターネット経由で情報を照会して返したり、サービスを起動したりするために使用できる。

スタンバイ・システム (standby system)
アクティブ・システムで障害が発生したときに、自動的にアクティブになるシステム。ディスクの複製が有効になっている場合は、アクティブ・システムからデータを複製する。

サブネット (subnet)
サブネットワーク (subnetwork) を参照。

サブネット・マスク (subnet mask)
インターネット・サブネットワークで、IP アドレスのホスト部分のサブネットワーク・アドレス・ビットの識別に使用される 32 ビットのマスク。

サブネットワーク (サブネット) (subnetwork (subnet))
より小さい独立したサブグループに分割されているが、相互接続された状態にあるネットワーク。

サブ検索 (sub-search)
完了した検索結果セット内で検索照会を実行できるようにする機能。

スーパーフロー (superflow)
ストレージの制約を減らすことによって処理能力を上げるための、類似するプロパティーを持つ複数のフローから構成される単一のフロー。

システム・ビュー (system view)
システムを構成するプライマリー・ホストと管理対象ホストの両方の視覚的な表現。

T

TCP 伝送制御プロトコル (Transmission Control Protocol) を参照。

伝送制御プロトコル (TCP) (Transmission Control Protocol (TCP))
インターネット、および Internet Engineering Task Force (IETF) のインターネットワーク・プロトコル標準に準拠するネットワークで使用される通信プロトコル。TCP は、パケット交換通信ネットワークと、そのようなネットワークの相互接続システムで、信頼できるホスト間プロト

コルを提供する。インターネット・プロトコル (Internet Protocol) も参照。

トラストストア・ファイル (truststore file)
トラステッド・エンティティーの公開鍵が入っている鍵データベース・ファイル。

V

違反 (violation)
企業ポリシーをくぐり抜けたり、違反したりする行為。

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。

W

WHOIS サーバー (whois server)
ドメイン名や IP アドレスの割り振りなど、登録されているインターネット・リソースに関する情報の取得に使用されるサーバー。

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]

[ナ行]

[ハ行]

[ヤ行]

[ラ行]

Q

S

W