IBM Security QRadar Incident Forensics
バージョン 7.2.6

管理ガイド

IBM

注記

本書および本書で紹介する製品を使用する前に、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 V7.2.6 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 Incident Forensics
Version 7.2.6
Administration 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

IBM Security QRadar Incident Forensics 管理の概要

IBM® Security QRadar® Incident Forensics の管理に関する情報。

対象読者

管理者は、アクティブな Forensics 機能の作成、保守、および操作によって、ユーザー (調査担当者といいます) がセキュリティー・インシデント (ケース) の調査およびデータの検討に専念できるようにします。

技術資料

すべての翻訳資料を含む IBM Security QRadar 製品資料を Web で見つけるには、IBM ナレッジ・センター(http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。

QRadar 製品ライブラリーでより技術的な資料にアクセスする方法については、Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644) 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方法については、Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144) 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。

注意:

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。

注記

IBM Security QRadar Incident Forensics は、企業によるセキュリティー環境とデータの改善の支援を目的として設計されています。具体的には、IBM Security QRadar Incident Forensics は、企業がネットワーク・セキュリティー・インシデントで何が起きたのかを調査およびより詳細に把握できるように設計されています。本ツールを使用することにより、企業は収集済みのネットワーク・パケット・データ (PCAP) に索引を付けて検索することができ、また本ツールにはそのようなデータを元の形式に再構成する機能が組み込まれています。この再構成機能により、電子メール・メッセージを含むデータおよびファイル、添付ファイルおよび添付画像、VoIP 通話、ならびに Web サイトを再構成することができます。本プログラムの機能および構成方法に関する追加情報が、本プログラムに付属するマニュアルおよびその他の資料に記載されています。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 Incident Forensics 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 Incident Forensics 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 Incident Forensics V7.2.6 の管理に関する新機能

IBM Security QRadar Incident Forensics V7.2.6 では、より多くのプロトコル、Web ドメイン、およびファイル・タイプを識別する新規の Inspector が導入されます。管理者は、ユーザーおよびシステムの使用状況を監査することもできます。

QRadar Incident Forensics で、より多くのプロトコル、Web ドメイン、およびファイル・タイプを処理できる

より多くの Inspector がサポートされるようになりました。これにより、パケット・キャプチャー (PCAP) ファイルおよびアップロードされた文書内の複数のプロトコル、Web ドメイン、およびファイル・タイプを識別できます。

SPDY 開発された Web コンテンツをトランスポートするために使用されるオープン・ネットワーク・プロトコルです。これにより、Web ページをロードするためにかかる時間を削減し、Web セキュリティーを向上させることができます。

Samba (SMB)
Server Message Block (SMB) は、コンピューター間でファイル、プリンター、シリアル・ポート、および名前付きパイプやメール・スロットなどの通信を共有するためのプロトコルです。バージョン 1 がサポートされています。

Web アプリケーション分類 (WAC)
QRadar Incident Forensics は、URL を検査し、Web アプリケーションおよび操作のタイプを識別することができます。その後、この情報を使用して、Web アプリケーションおよび操作に基づいて、トラフィックをクラスに分類します。

QFlow アプリケーション検出
QFlow アプリケーション検出は、他の Inspector がアプリケーション、セッション、またはプロトコルを検出できない場合に使用されます。QFlow アプリケーション検出は、パケットの最初の 64 バイトでシグニチャーを検査し、シグニチャーとポートからアプリケーションを識別しようとします。

詳細...

ユーザーとアプリケーションのアクティビティーを追跡および記録するための監査ログ

監査ログは、セキュリティー・アナリストの作業内容 (アナリストが実行しているアクション、アクセスしているデータ、および表示している情報) を可視化します。調査内で実行された一連のアクティビティーが文書化され、証拠として記録されます。

監査ログ・イベントを生成するアクティビティーは次のとおりです。

- ケースの作成
- ケースの削除
- コレクションの削除
- すべてのユーザー照会
- 文書表示
- 文書のエクスポート

詳細...

第 2 章 Forensics 機能の管理ワークフローとユーザー・アクセス

IBM Security QRadar Incident Forensics をインストールして構成すると、管理者はシステムとその動作についてトラブルシューティング、保守、モニターを行うことができます。また、ケースへのユーザー・アクセスを管理することもできます。

QRadar Incident Forensics の管理ツールを表示するには、管理特権が必要です。

例: 管理ワークフロー

QRadar Incident Forensics の管理のサンプル・ワークフローを以下のダイアグラムに示します。

1. サーバー管理を使用して、モニター対象にしない Web カテゴリーとトラフィックをフィルターに掛けます。
2. Forensics ユーザー権限を使用してケースを調査担当者に割り当てます。
3. ケース管理を使用してケースの作成と削除を行い、外部のコンテンツをシステムにインポートします。
4. スケジュール済みアクションを使用して、古い文書の削除、データベースのチューニング、QRadar Incident Forensics サーバーのリセットなどの保守をスケジュールします。

ユーザー・ロール

ユーザー・アカウントを追加するには、ユーザーの特定のアクセス要件を満たすために、まずセキュリティー・プロファイルを作成する必要があります。セキュリティー・プロファイル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。

QRadar の「**管理**」タブの「ユーザー・ロール」ツールで、以下のユーザー・ロールを割り当てることができます。

管理
ユーザーは、ユーザーおよびすべてのインシデントに割り当てられているすべてのケースを表示してアクセスすることができ、自動的に QRadar Incident Forensics のフルアクセスを付与されます。

Forensics
ユーザーは「**Forensics**」タブを表示してアクセスすることはできますが、ケースを作成することはできません。

Incident Forensics でのケースの作成
ユーザーは自動的に Forensics ケースを作成できます。

第 3 章 サーバー管理

管理者は IBM Security QRadar Incident Forensics システムとその動作についてトラブルシューティング、保守、モニターを行うことができます。

サーバー設定をモニターまたは変更する場合、あるいはシステムにログインしているユーザーを表示する場合は、以下の手順でサーバー管理ツールを開きます。

1. 管理者として QRadar にログオンします。
2. 「**管理**」タブをクリックします。
3. メインペインの「**Forensics**」セクションで、「**サーバー管理**」をクリックします。

サーバー構成設定値

IBM Security QRadar Incident Forensics サーバー管理ツールのサーバー設定を使用して、すべての管理対象ホストに影響を及ぼすシステム設定を構成します。設定を変更した後、「**管理**」タブの「**変更のデプロイ**」メニューを使用して、変更をデプロイする必要があります。

ログアウト時に検索履歴をクリア
ユーザーがログアウトするときに検索履歴をクリアします。検索のクリアは、Query Helper の照会履歴リストと、「検索と結果 (Search and Results)」ページの「**検索条件の入力 (Search Criteria Input)**」フィールドの最後のユーザーに適用されます。

視覚化するノードのデフォルト数
視覚化ツールに表示するノードの最大数。表示するノードの数は、初回の表示後に構成することができます。表示するノードの数を調整しても、影響が及ぶのは視覚化ツールの対象インスタンスのみです。

Protocol Inspector および Domain Inspector のフィルター

サーバー管理ツールで Protocol Inspector または Domain Inspector を非アクティブにすることで、特定のタイプのトラフィックを調査から除外できます。「**インスペクター・フィルター (Inspector Filter)**」オプションを使用します。

Protocol Inspector および Domain Inspector は、取り込んだネットワーク・トラフィック・データを処理し、有意義な方法でデータの識別および索引付けを試みます。データの識別と索引付けにより、調査担当者が、情報の検索をより正確にコントロールできます。

ネットワーク・トラフィック・データが取り込まれ、プロトコルが識別されると、そのデータは適切な Protocol Inspector によってさらに検査されます。HTTP Protocol Inspector によって識別されたネットワーク・トラフィック・データは、さらに Domain Inspector によって検査され、索引が付けられます。

Protocol Inspector

Protocol Inspector は、HTTP、POP3、FTP、および Telnet などのプロトコルを識別することができます。Protocol Inspector を除外できます。Inspector を除外しても、その Inspector に関連するネットワーク・トラフィック・データはすべて取り込まれますが、トラフィックの識別と索引付けは一般的なレベルでのみ行われます。

Domain Inspector

Domain Inspector は特定の Web サイトを検査します。Domain Inspector を除外できます。 Domain Inspector を除外しても、その Inspector に関連する HTTP ネットワーク・トラフィック・データはすべて取り込まれますが、トラフィックの識別と索引付けは HTTP レベルでのみ行われます。 Domain Inspector をアクティブにするには、HTTP Protocol Inspector もアクティブにする必要があります。

デフォルトでは、すべてのフィルターがオンになっており、すべてのプロトコルのトラフィックを表示できます。唯一の例外は SIP (Session Initiation Protocol) トラフィックです。この呼設定プロトコルは、アプリケーション層で作動するため、デフォルトではオフになっています。

要確認: Inspector のフィルターの構成を変更すると、新規構成は、作成されるすべての新規ケースに適用されます。オンになっている Inspector は、ケースに対して作成される文書に影響し、調査担当者は、特定の Inspector について検索の機能を使用できなくなります。ユーザーには、どの Inspector がケースに適用されているかは分かりません。

Inspector によって処理されないプロトコルは、不明として分類されます。

Web カテゴリー・フィルター

Web カテゴリー・フィルターを使用して、認識される Web ページおよび Web サーバーのタイプを選択できます。

例えば、特定のタイプの HTTP ネットワーク・トラフィックを調査から除外できます。HTTP ネットワーク・トラフィックのデータを取り込むときに、データは分類され、得られた文書はグループ化されます。

管理者は、HTTP ネットワーク・トラフィック・データをフィルターに掛けて、データが取り込まれることを防ぐことができます。

あるカテゴリーまたはグループについてトラフィックを除外またはフィルターに掛けるには、サーバー管理ツールでそのカテゴリーまたはグループをオフにします。

Web カテゴリー化、グループ化、およびフィルター処理は、HTTP ネットワーク・トラフィック・データが取り込まれる際に作用します。既にシステムに存在するデータには影響を及ぼしません。

データを除外するようにグループ・フィルターを設定すると、そのグループのカテゴリーに関連付けられている HTTP ネットワーク・トラフィック・データは、関連するカテゴリー・フィルターの設定に関わらず、コンシューム中にフィルターに掛けられて除外されます。

例: Web カテゴリー・フィルターを使用してトラフィックを除外した場合

ニュース・サイトまたはマガジン・サイトからのデータを含むトラフィックを除外することにします。

1. QRadar の「**管理**」タブで、「**サーバー管理**」をクリックします。
2. 「**Web カテゴリー・フィルター (Web Category Filter)**」をクリックし、「**ニュース/マガジン (News / Magazines)**」フィルターの横にある「**オフ (Off)**」をクリックします。
3. 「**Web メール/ユニファイド・メッセージング (Webmail / Unified Messaging)**」フィルターをクリックし、「**オン (On)**」をクリックします。

これで、ユーザーは「**Forensics**」タブ上で取り込まれたトラフィックを調べてみると、「**Web メール/ユニファイド・メッセージング (Webmail / Unified Messaging)**」フィルターがオンであっても、「**ニュース/マガジン (News / Magazines)**」データと「**Web メール/ユニファイド・メッセージング (Webmail / Unified Messaging)**」データの両方を含むトラフィックは取り込まれていないことが分かります。

サポートされるプロトコルおよび文書タイプ

IBM Security QRadar Incident Forensics は、ネットワーク・フローのパケットおよび索引のコンテンツをキャプチャーし、ペイロードおよびメタデータを処理します。

以下に、QRadar Incident Forensics で処理可能なサポートされるプロトコルをリストします。

- AIM
- DHCP
- DNS
- Exchange
- FTP
- HTTP
- IMAP
- IRC
- Jabber
- Myspace
- NFS
- SIP
- NetBIOS
- Oracle
- POP3
- SMB
- SMTP

- SPDY
- TLS (SSL)
- SSH
- Telnet
- Yahoo Messenger
- MySQL

以下に、QRadar Incident Forensics で処理可能なサポート・ドメイン (Web サイト) と、そのドメインでサポートされる言語をリストします。

- AOL (Accessible、Basic、Standard) (EN)
- Charter (EN)
- Facebook (Mobile、Desktop) (AR、CN、DE、EN、ES、FR、RU)
- Gmail (Classic、Standard) (AR、CN、DE、EN、ES、FR、RU)
- Hotmail (AR、CN、DE、EN、ES、FR、RU)
- LinkedIn (DE、EN、ES、FR、RU)
- MailCom (CN、EN、ES、FR、RU)
- MailRu (RU)
- Maktoob (AR、EN)
- Myspace (EN)
- QQMail (EN、CN)
- Twitter (EN)
- YAHOO メール (Standard、Classic) (EN)
- YAHOO Note (EN)
- YouTube (AR、CN、DE、EN、ES、FR、RU)
- Comcast (Zimbra) (EN)

以下に、QRadar Incident Forensics で処理可能なサポートされる文書フォーマットをリストします。

- ハイパーテキスト・マークアップ言語
- XML および派生フォーマット
- Microsoft Office 文書フォーマット
- OpenDocument フォーマット
- PDF フォーマット
- Electronic Publication フォーマット
- リッチ・テキスト・フォーマット
- 圧縮フォーマットおよびパッケージング・フォーマット
- テキスト・フォーマット
- オーディオ・フォーマット
- イメージ・フォーマット
- ビデオ・フォーマット
- Java™ クラス・ファイルおよびアーカイブ

- mbox フォーマット

QFlow アプリケーション検出

QFlow アプリケーション検出は、他の Inspector がアプリケーション、セッション、またはプロトコルを検出できない場合に使用されます。QFlow アプリケーション検出は、パケットの最初の 64 バイトでシグニチャーを検査し、シグニチャーとポートからアプリケーションを識別しようとします。QFlow アプリケーション検出が識別できる可能性があるアプリケーション、セッション、またはプロトコルのいくつかの例を以下に示します。ただし、以下の項目のみに限定されるものではありません。

- BitTorrent
- Blubster
- CitrixICA
- Google Talk
- Gnucleuslan
- Gnutella
- GSS-SPNEGO
- NTLMMSSP
- OpenNap
- PeerEnabler
- Piolet
- UpdateDaemon
- VNC

第 4 章 ケース管理

管理者は、ケース管理を使用して、ケースとコレクションを管理できます。文書およびパケット・キャプチャー (pcap) ファイルのコレクションについてケースを作成できます。また、外部ファイルを IBM Security QRadar Incident Forensics システムにインポートできます。

ケース管理のチューニング

ケース管理をチューニングするには、「**フラッシュ (Flush)**」オプションを使用します。*pcap* ストリーミング・データ (一連の pcap ファイルであり、論理的に関連付けられて 1 つの大きい pcap ファイルを形成する) の場合、バッファリングしたデータを強制的にディスクに書き込むことができます。「**フラッシュ (Flush)**」オプションを使用すると、QRadar Incident Forensics ホストは、終了していないフローを強制的にディスクに書き込みます。これは、初期段階でこれらのフロー内を検索するために役立ちます。

分布グラフ

ケースの削除を予定している場合、グラフを使用して視覚的かつ迅速にケースのコンテンツを確認できます。ケース内のファイルのタイプ、プロトコル、およびドメインを確認できます。

管理対象ホストへの pcap ファイルのアップロード

pcap データを外部ソースから手動でアップロードできます。処理のためにデータをアップロードする QRadar Incident Forensics 管理対象ホストを指定することができます。例えば、3 つの管理対象ホストと 3 つの pcap ファイルがある場合、それぞれのファイルを別々の管理対象ホストにアップロードできます。大きな pcap ファイルの場合は、FTP を使用してください。

ケースの作成

ケースとは、インポートした文書や pcap ファイルを集積するための論理的なコンテナーのことです。すべての pcap ファイルに対して 1 つのケースを使用することも、複数のケースを作成することもできます。ケースは特定のユーザーに制限することができます。

手順

1. 「**管理**」タブで「**ケース管理**」を選択します。
2. 「**新規追加 (Add New)**」をクリックします。
3. 「**ケース名 (Case Name)**」フィールドに、固有の名前を入力します。

   制約事項: ケース名にスペースを使用することはできません。
4. 「**保存**」をクリックします。

タスクの結果

ケース名に基づく新規ディレクトリー /case_input/<*case_name*> が作成されます。このディレクトリーは pcap ファイルのインポートに使用します。

ケースへのファイルのアップロード

管理者は、外部パケット・キャプチャー (pcap) ファイルや、スプレッドシート、テキスト・ファイル、イメージ・ファイルなどの文書を IBM Security QRadar Incident Forensics ケース管理にアップロードできます。

以下のファイル・タイプがサポートされます。

- ハイパーテキスト・マークアップ言語
- XML および派生フォーマット
- Microsoft Office 文書フォーマット
- OpenDocument フォーマット
- PDF フォーマット
- Electronic Publication フォーマット
- リッチ・テキスト・フォーマット
- 圧縮フォーマットおよびパッケージング・フォーマット
- テキスト・フォーマット
- オーディオ・フォーマット
- イメージ・フォーマット
- ビデオ・フォーマット
- Java クラス・ファイルおよびアーカイブ
- mbox フォーマット

ケース管理では、ケースに追加できるファイルの数と最大ファイル・サイズの両方に制限があります。

手順

1. 「**管理**」タブの「**Forensics**」 セクションで、「**ケース管理**」をクリックします。
2. ケースを選択します。
   - 既存のケースに外部のファイルを追加するには、「**ケース**」リストからケースを選択します。
   - 新規ケースにファイルを追加するには、「**新規追加 (Add New)**」をクリックします。

     制約事項: ケース名にスペースを使用することはできません。
3. 「**ホストへのアップロード (Upload to Host)**」リストから、ファイルを処理する管理対象ホストを選択します。
4. pcap ファイルまたはその他の文書タイプを追加するには、次のいずれかの方法を選択します。

- 「**pcaps の追加 (Add pcaps)**」をクリックし、ファイルを選択して、「**アップロードの開始 (Start upload)**」をクリックします。
- ファイルをアップロード・ボックスにドラッグします。

アップロードが完了すると、ファイルが「**コレクション**」リストにリストされます。

第 5 章 ユーザーへのケースの割り当て

管理者は、Forensics データへのアクセス権をユーザーに付与し、ユーザーにケースを割り当て、FTP アクセス権などのユーザー権限を構成します。ユーザーはケースを割り当てられるまではデータを表示できず、割り当てられたケースからのデータしか表示できません。

ネットワークへのアクセスを制限されている非管理ユーザーにケースを割り当てるときは、注意が必要です。これらのユーザーは、通常はアクセスできない IP アドレスからの文書を表示できます。例えば、財務情報または人事情報が含まれるケースを非管理ユーザーに割り当てた場合、そのユーザーはケースを調査するときにデータを表示できます。

このタスクについて

管理者は以下のタスクを実行できます。

- ケースへの複数ユーザーの割り当て
- ユーザーからのケースの削除
- ユーザーに割り当てられているすべてのケースの表示とそれらのケースへのアクセス

ユーザーが表示できるケースは、そのユーザーに明示的に割り当てられているケースのみです。

手順

1. 「**管理**」タブで「**Forensics ユーザー権限**」をクリックします。
2. 「**ユーザー**」リストからユーザーを選択します。
3. 「**使用可能**」リスト内のケース・リストから、1 つ以上のケースを選択し、矢印 (>) をクリックして、そのケースを「**割り当て済み**」リストに移動します。

   ヒント: デフォルトでは、管理特権を持つユーザーはすべてのケースに割り当てられます。左矢印 (<) および右矢印 (>) は表示されません。

Forensics ケースへの手動によるファイルのインポート

ケース管理ツールとは異なり、手動でファイルをインポートする場合は、ファイル・サイズおよびファイル数に制限はありません。ケースを手動で作成してそれにファイルをコピーすることも、既存のケースに手動でファイルをコピーすることもできます。

例えば、**scp** コマンドを使用して、別のホストから IBM Security QRadar Incident Forensics ホスト上の `/opt/ibm/forensics/case_input/case_input/` ディレクトリーにファイルを安全にコピーすることができます。

始める前に

インポートしたファイルのバックアップ・コピーを作成します。ファイルのインポートと処理が完了すると、元のファイルは削除されます。

手順

1. SSH を使用して QRadar Incident Forensics に root ユーザーとしてログインします。
2. 新規ケースを作成するには、/opt/ibm/forensics/case_input に移動して以下のコマンドを入力します。

   ```
   mkdir /opt/ibm/forensics/case_input/<case_name>
   ```

3. ケースにファイルをコピーするには、**scp** コマンドまたはその他のファイル転送プログラムを使用して、ファイル・タイプに対応するディレクトリーにファイルをコピーします。

   インポートしたファイルのディレクトリー構造を以下の表に示します。

表 1. ケース・ファイルのディレクトリー構造

ディレクトリー	説明
/opt/ibm/forensics/case_input/<*case_name*>	一連の pcap または連結したストリームの pcap ファイルをインポートするために使用するディレクトリー。
/opt/ibm/forensics/case_input/<*case_name*>/singles	個々の pcap ファイルをインポートするために使用するディレクトリー。
/opt/ibm/forensics/case_input/case_input/<*case_name*>/import	pcap 以外のタイプの単一ファイル (例えば、Microsoft Word 文書、Adobe Acrobat PDF、テキスト・ファイル、イメージなど) をインポートするために使用されるディレクトリー。

   重要: ファイル名にハイフンを使用すると、ファイルのインポート時にハイフンが下線に変更されます。

タスクの結果

インポートに成功すると、作成したケースの「コレクション」ウィンドウにファイル名が自動的に表示されます。

外部システムから Forensics ケースへの pcap ファイルおよび文書の FTP をユーザーに許可

外部データをアップロードして特定のケースに含めるために、管理者はセキュア FTP の権限をユーザーに付与して、そのデータが関連付けられているケースを管理できます。ユーザーは、FTP 要求を処理する IBM Security QRadar Incident Forensics ホストを選択できます。

FTP アクセスが有効になった後でパスワードを変更するには、FTP アクセスを無効にし、ユーザーを保存してから、FTP アクセスを再度有効にし、新規パスワードを入力する必要があります。

始める前に

「**管理**」タブのユーザー・ロール・ツールで、Forensics 調査担当者のロールを作成するか、割り当てておきます。

デフォルトでは、`/etc/vsftpd/vsftpd.conf` ファイルは、55100 から 55104 までの 5 つのポートが開くように構成されています。ポート範囲を変更するには、`/etc/vsftpd/vsftpd.conf` ファイルを編集して、`pasv_min_port` および `pasv_max_port` 設定の値を、希望するポート範囲に変更します。「**管理**」タブの「**変更のデプロイ**」をクリックして、構成の変更をデプロイする必要があります。

このタスクについて

IBM Security QRadar Incident Forensics では、ネットワーク上のアクセス可能な任意のディレクトリーからデータをインポートできます。さまざまなフォーマットのデータをインポートできます。そのようなフォーマットには以下が含まれますが、これらには限定されません。

- 外部ソースからの標準 PCAP フォーマットのファイル
- テキスト・ファイル、PDF ファイル、スプレッドシート、プレゼンテーションなどの文書
- イメージ・ファイル
- アプリケーションからのストリーミング・データ
- 外部 PCAP ソースからのストリーミング・データ

ユーザーは 1 つのケースに複数のファイルをアップロードでき、管理者は複数のユーザーにケースへのアクセス権を付与できます。

制約事項: ケース名は一意である必要があります。1 つのケースには単一のユーザーが関連付けられているため、2 人のユーザーが同じ名前のケースを作成することはできません。

手順

1. 「**管理**」で「**Forensics ユーザー権限**」をクリックします。
2. 「**ユーザー**」リストからユーザーを選択します。
3. 「**ユーザーの編集 (Edit User)**」ペインで、「**FTP アクセスを許可 (Enable FTP access)**」チェック・ボックスを選択します。
4. ユーザーの FTP パスワードを入力し、確認します。
5. 「**ユーザーの保存 (Save User)**」をクリックして、権限に対する変更を保存します。
6. FTP クライアントで、以下の手順を実行します。
   a. プロトコルとしてトランスポート層セキュリティー (TLS) が選択されていることを確認します。
   b. QRadar Incident Forensics ホストの IP アドレスを追加します。

c. 作成された QRadar Incident Forensics ユーザー名とパスワードを使用するログオンを作成します。

7. QRadar Incident Forensics サーバーに接続して、新規ディレクトリーを作成します。
8. pcap ファイルに対して FTP を実行して保管するために、ケース用に作成したディレクトリーの下に `singles` という名前のディレクトリーを作成して、そのディレクトリーに pcap ファイルをドラッグします。
9. pcap ファイル以外の他のファイル・タイプに対して FTP を実行して保管するために、ケース用に作成したディレクトリーの下に `import` という名前のディレクトリーを作成して、そのディレクトリーにそれらのファイルをドラッグします。
10. FTP サーバーを再始動するために以下のコマンドを入力します。

```
etc/init.d/vsftpd restart
```

11. ファイルをアップロード領域から QRadar Incident Forensics ディレクトリーに移動するサーバーを再始動するために、以下のコマンドを入力します。

```
/etc/init.d/ftpmonitor restart
```

タスクの結果

管理者には、ケース管理にアップロードされたデータが表示されます。ユーザーは、「**Forensics**」タブのいずれかのツールに自分のケースを表示できます。

QRadar Incident Forensics での SSL および TLS トラフィックの復号

隠れた脅威を検出するために、IBM Security QRadar Incident Forensics では SSL トラフィックを復号できます。サーバーの秘密鍵と IP アドレス、またはブラウザーのセッション鍵とその他のセッション情報を提供すると、Protocol Inspector は SSL トラフィックを復号できます。

セッション鍵が外部サイトから生成された場合、または別のブラウザーによって生成された場合は、Protocol Inspector はブラウザー・セッションから SSL トラフィックを復号できません。

制約事項: `Diffie Hellman` 鍵交換メカニズムは、暗号化されたトラフィックが秘密鍵によって復号される場合はサポートされません。秘密鍵を使用する場合は、RSA など他の鍵交換方式がサポートされています。

トラフィックが keylog 内の情報を使用して復号される場合、`Diffie Hellman` の制限は適用されません。

このタスクについて

復号は次のプロトコルでサポートされます。

- SSL v3
- TLS v1.0
- TLS v1.1
- TLS v1.2

鍵ログ・ファイルは、Chrome、Firefox、および Opera の各ブラウザーによって SSLKEYLOGFILE 環境変数を使用して生成されます。SSLKEYLOGFILE セッション鍵では、以下の鍵フォーマットがサポートされます。

- RSA
- DH

手順

1. SSH を使用して QRadar Incident Forensics プライマリー・ホストに root ユーザーとしてログインします。
2. /opt/qradar/forensics.conf ファイルで鍵の場所を確認します。

   ```
   <sslkeys
   keydir="/opt/ibm/forensics/decapper/keys"
   keylogs="/opt/ibm/forensics/decapper/keylogs"/>
   ```

3. /opt/qradar/forensics.conf ファイルに指定されているディレクトリーに鍵をコピーします。
   - 秘密鍵の場合は、鍵を /opt/ibm/forensics/decapper/keys ディレクトリーにコピーします。

     例:

     ```
     <keys>
      <key file=" /opt/ibm/forensics/decapper/keys/key_name">
         <address> 1.2.3.4</address>
         <range> 1.2.3.0-1.2.3.255</range>
       </key></keys>
     ```

   - ブラウザーによって生成された鍵ログ・ファイルの場合は、その鍵ログ・ファイルを /opt/ibm/forensics/decapper/keylogs/default ディレクトリーにコピーします。

   /opt/ibm/forensics/decapper/keys ディレクトリーまたは /opt/ibm/forensics/decapper/keylogs ディレクトリー内のサブディレクトリーを変更する場合は、decapper サービスを再始動する必要があります。

   decapper サービスを再始動するには、次のコマンドを入力します。service decapper restart

第 6 章 QRadar Incident Forensics でのスケジュール済みアクション

古い文書の削除、データベースのチューニング、IBM Security QRadar Incident Forensics サーバーのリセットなどの保守をスケジュールできます。

大量の文書がある場合は、古い文書の削除などのスケジュールされたアクションの完了に時間がかかることがあります。ケース全体を削除する場合は、ケース管理ツールを使用します。

文書の削除

管理者は、文書のネットワーク・タイム・スタンプに基づいて、古くなった文書を削除することができます。

pcap ファイルおよびその他のタイプのファイルなどの文書をケースまたはサーバーから削除できます。古くなった文書を削除すると、文書を検索するときの速度を維持するのに役立ちます。

ケースのフラッシュ

ケース管理をチューニングするには、「**ケースのフラッシュ (Flush Case)**」オプションを使用します。*pcap* ストリーミング・データ (一連の pcap ファイルであり、論理的に関連付けられて 1 つの大きい pcap ファイルを形成する) の場合、バッファリングしたデータを強制的にディスクに書き込むことができます。「**ケースのフラッシュ (Flush Case)**」オプションを使用すると、QRadar Incident Forensics ホストは、終了していないフローを強制的にディスクに書き込みます。これは、初期段階でこれらのフロー内を検索するために役立ちます。

データベースの最適化

管理者は、データベースを最適化して、検索エンジンの索引をセグメントに再編成したり、削除された文書を除去したりすることができます。

「**データベースの最適化**」スケジュール済みアクションは **defrag** コマンドに似ています。

データベースを最適化すると、新規索引が作成されます。索引が作成されると、新規索引で古い索引が置き換えられます。古い索引が置き換えられるまでは 2 つの索引が存在するため、索引最適化コマンドを実行するには 2 倍の量のハード・ディスク・スペースが必要です。

データベースを最適化する前に、索引のサイズがハード・ディスクの使用可能スペースの 50% を超えていないことを必ず確認してください。

QRadar Incident Forensics ホストのアクションのスケジュール

IBM Security QRadar Incident Forensics ホスト上の保守タスクをスケジュールできます。

次のタスクをスケジュールできます。

- 現在使用可能なケースの新規索引を作成する。
- 指定された期間後には保持しない文書を削除する (エージ・アウト)。
- データを強制的にディスクに書き込む。

手順

1. 「**管理**」タブの「**Forensics**」セクションで、「**アクションのスケジュール**」をクリックします。
2. 「**新規アクションの追加 (Add New Action)**」をクリックします。
3. 「**アクションの選択 (Select Action)**」リストから、アクションを選択し、設定を指定します。
   - 現在のケースの新規索引を作成するには、「**索引の最適化 (Optimize Index)**」を選択します。

     新規索引には、既存の索引の約 2 倍のスペースが必要です。十分なスペースがあることを確認してください。
   - 指定された存続期間より古いネットワーク・タイム・スタンプを持つ文書を削除するには、「**文書のエージ・アウト (Age Out Documents)**」を選択します。

     文書を削除するときには、索引も削除されます。
   - 終了していないフローをディスクに書き込むには、「**ケースのフラッシュ (Flush Case)**」を選択します。
4. 「**保存**」をクリックします。
5. アクションを実行、編集、または削除するには、「**アクション**」リストのアクションを選択し、「**実行**」、「**編集**」、または「**削除**」をクリックします。

第 7 章 QRadar Incident Forensics でのユーザーおよびシステムの使用状況の監査

監査ログは、データ・アクセスに関連付けられているユーザー・アカウントを識別する日時順レコードです。これらのログは、通常とは異なるアクセスまたは無許可アクセスを検出でき、失敗したジョブなどの問題を識別できます。

監査ログ・イベントを生成するアクティビティーは次のとおりです。

- ケースの作成
- ケースの削除
- コレクションの削除
- すべてのユーザー照会
- 文書表示
- 文書のエクスポート

制約事項: コレクションの作成イベントのロギングはサポートされていません。

手順

1. SSH を使用して QRadar コンソールまたは QRadar Incident Forensics Standalone に管理者としてログオンします。
2. `/var/log/audit` ディレクトリーに移動します。
3. vi などのエディターで `audit.log` ファイルを開いてコンテンツを確認するか、**`grep`** コマンドを使用して特定の項目を検索します。

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。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

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。