IBM Security QRadar Incident Forensics
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使用する前に、41 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
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

目次

IBM Security QRadar Incident Forensics 使用ガイド

このガイドには、IBM® Security QRadar® Incident Forensics を使用したセキュリティー・インシデントの調査に関する情報が含まれています。

対象読者

調査担当者は、Forensics リポジトリーにあるネットワーク・トラフィックや文書から情報を抽出します。セキュリティー・インシデントの調査ではこの情報を使用します。

技術文書

IBM Security QRadar の製品資料 (すべての翻訳資料を含む) を Web 上で探すには、IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。

QRadar 製品ライブラリー内の技術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対策に関する注意事項

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。このツールにより、企業は、キャプチャーしたネットワーク・パケット・データ (PCAP) に索引を付けて検索し、該当するデータを元の形に再構成できる機能を組み込むことができます。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。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 のユーザー用の新機能

IBM Security QRadar Incident Forensics V7.2.6 には、疑わしいコンテンツや動作についてファイルや画像を分析するのに役立つ新しい調査ツールが導入されています。Web ページと共謀者の間の関係やつながりを示すリンクも分析することができます。

疑わしいコンテンツや悪質なコンテンツについての成果物分析

成果物分析を使用して、システムがどのように感染したのか、および他の資産が同様に危殆化しているかどうかなど、インシデントを調査できます。

例えば、復元されたパケット・データにファイル分析機能を使用して、すべてのファイルのリストと、それらのファイルに埋め込みのファイルやスクリプトが含まれているかどうかを確認することができます。

疑わしいコンテンツや埋め込みスクリプトがあるとしてフラグが立てられた画像ファイルを調べることができます。

ファイルのエントロピー・スコアおよびエントロピー分布は、ファイルの異常を識別するのに役立ちます。そしてそのファイルに、検出から逃れて、システムが感染する原因となったマルウェアが含まれることの証拠を提供します。

他のどのシステムが影響を受けている可能性があるかを判別するために、リンク分析を使用して、閲覧されたすべての Web サイトと、感染した Web ホストへのアクセスのサブセットを素早く可視化することができます。

詳細...

第 2 章 セキュリティーの調査

IBM Security QRadar Incident Forensics を使用すると、新種の脅威を検出し、根本原因を判別して、再発を防止することができます。 Forensics ツールを使用することにより、誰が脅威を起こしたか、それがどのように実行され、何が危殆化したかについての分析に迅速に焦点を当てることができます。

フォレンジック調査担当者は、サイバー犯罪のステップバイステップのアクションを再トレースし、セキュリティー・インシデントに関連した生のネットワーク・データを再構成することができます。

組織が最初に脅威やセキュリティー・リスクまたはコンプライアンス違反の可能性を認識したときに、調査担当者は、目的を設定して範囲を評価し、関与しているエンティティーを特定し、動機付けを把握します。

ネットワーク・セキュリティー、内部者分析、不正と濫用、および証拠収集などの各種調査の具体的なシナリオで、IBM Security QRadar Incident Forensics のツールを使用できます。

1. IP アドレスとの間のネットワーク・セッションをリカバリーおよび再構成します。
2. 作成されたインシデントから、証拠を収集するために属性のカテゴリーを照会できます。

   リカバリーを作成すると、インシデントが作成されます。
3. 検索フィルターを使用して、関心のある情報のみを取得します。
4. 調査のタイプに応じて、必要な証拠を提供する Forensics ツールを選択します。

疑わしいコンテンツ

検索を使用すると、攻撃者やインシデントについて把握しているコンテキストのエレメントまたは ID を見つけることができます。 検索でキーワードを使用すると、疑わしいコンテンツが返されます。一部の疑わしいコンテンツは、調査に関連している場合があります。

データのピボット操作

データのピボット操作は、検索結果で返されたコンテンツをホット・リンクとして表示することにより実現します。例えば、「Tom」を検索すると、その結果には Tom が作成した E メール、Tom のチャット、およびその他のコンテキスト情報が含まれる場合があります。 E メールをクリックして表示すると、Tom が使用した各アセットまたはエンティティー (添付ファイルやコンピューター ID など) がリンクとして表示されます。調査担当者は、これらのリンクを使用して、迅速な調査を行うことができます。

デジタル・インプレッション

デジタル・インプレッションを使用して、データを参照し、頻度に基づいて IP アドレス、名前、および MAC アドレスなどのエンティティー間の関係をマップします。 1 つ以上の結果を選択して、関係の頻度と方向を表示できます。

Surveyor

Surveyor を使用して、アクティビティーのタイムラインを表示し、攻撃を再トレースできるようにします。Surveyor はセッションを再構成し、文書を時間順にソートします。

コンテンツ・フィルタリング

コンテンツ・フィルタリングを使用すると、Web メール、ポルノなどのコンテンツ・カテゴリーのサブセットを参照し、ノイズや検索時に無関係なものを除去するのに役立ちます。

ネットワーク・セキュリティーの調査

QRadar Incident Forensics を使用すると、重要なアセットをターゲットとした悪意のあるアクティビティーを検出して調査することができます。組み込みの Forensics ツールを使用すると、ネットワーク・セキュリティー・ブリーチ (抜け穴) の修復に役立てることができ、またその再発を予防できます。

QRadar Incident Forensics の調査ツールは、イベントがどのように発生したかを把握し、その影響を最小化し、別の侵害を防ぐためのあらゆる措置を講じるのに役立ちます。

最初に感染したマシン: 攻撃元の特定

このシナリオでは、組織に対して、侵害の疑いがあるというアラートが出されます。組織は、感染源を隔離するために、最初の攻撃地点を見つけようとします。組織は、攻撃が組織内の他の部署に広がらないように、危殆化したエンティティーを検疫する必要があります。

目的

これらの調査において問題を解決する上での組織の目的は、以下のとおりです。

- 攻撃のタイプを判別する。
- 脅威の最初のエントリー・ポイントを特定する。
- 悪意のあるペイロードに関する詳細を入手する。
- 悪意のあるペイロードがエントリー・ポイントを超えてどのようにして広まったかを把握する。

調査

「**Forensics**」タブのツールを使用して、調査に役立てます。

1. フリー・フォーム検索を使用して、悪意のあるペイロードに関連する症状を示す特徴を検索します。

2. コンテンツ・カテゴリーを使用して、調査に関係のないコンテンツをフィルターに掛けて除外します。
3. 本製品によってフラグが立てられている疑わしいコンテンツを検査します。
4. デジタル・インプレッションと可視化を使用して、悪意のあるペイロード、加害者、またはターゲットの広範な関係を調べます。
5. データのピボット操作を使用して、データ・リンケージを追跡し、最初に感染したマシンを特定します。
6. Surveyor を使用して、アクティビティーのタイムラインを表示し、攻撃を再トレースできるようにします。

危殆化したシステム

このシナリオでは、組織に対して、ウォータリング・ホール、フィッシング、ブルート・フォース、SQL インジェクションなどの高度なサイバー攻撃手法により、システムの 1 つ以上が危殆化したというアラートが出されます。

目的

これらの調査において問題を解決する上での組織の目的は、以下のとおりです。

- 組織内の危殆化の範囲を判別する。
- 各システムでの危殆化による運用リスクのタイプを把握する。
- クリーンアップ・アクティビティーと検出を逃れるために初期攻撃で実行された周辺的なアクションを明らかにする。

調査

「**Forensics**」タブのツールを使用して、調査に役立てます。

1. フリー・フォーム検索を使用して、悪意のあるペイロードまたは危殆化したアセットを検索します。
2. 本製品によってフラグが立てられている疑わしいコンテンツを検査します。
3. デジタル・インプレッションと可視化を使用して、危殆化したシステムから生じたエンティティー関係を調べます。
4. Surveyor を使用して、アクティビティーのタイムラインを表示し、攻撃を再トレースできるようにします。
5. フリー・フォーム検索、データのピボット操作、および疑わしいコンテンツを使用して、データ・カテゴリー間の矛盾や疑わしい対話を検出します。

無許可エンティティーに漏えいしたデータ

このシナリオでは、組織に対して、組織内の無許可エンティティーまたは外部の関係者に機密データが漏えいしたというアラートが出されます。

目的

これらの調査において問題を解決する上での組織の目的は、以下のとおりです。

- 漏えいしたデータの性質と量を判別する。
- 使用された手法を把握する。
- 加害者を明らかにする。

- 漏えい元を特定する。

調査

「**Forensics**」タブのツールを使用して、調査に役立てます。

1. フリー・フォーム検索を使用して、漏えいしたデータの ID を検索します。
2. 本製品によってフラグが立てられている疑わしいコンテンツを検査します。
3. データの再構成を確認することにより、漏えいした、または漏えいしているデータの範囲全体を確認します。
4. デジタル・インプレッションと可視化を使用して、関与しているすべてのエンティティー関係を調べます。
5. Surveyor を使用して、アクティビティーのタイムラインを表示し、攻撃を再トレースできるようにします。
6. フリー・フォーム検索を使用して、データ漏えいの動機付けを明らかにします。
7. データのピボット操作を使用して、漏えいした可能性のある他のデータとの関係を明らかにします。

内部者分析の調査

QRadar Incident Forensics を使用して、共謀、システム破壊、およびアクセス権限の誤用を検出します。加害者を特定し、コラボレーターを特定して、危殆化したシステム、および文書データの損失を特定します。

アクセス権限の誤用

このシナリオでは、組織に対して、1 人以上の従業員が資格情報を誤用しているか、その資格情報をプロキシーとして使用して、無許可のアクティビティーのために機密システムやデータにアクセスしているというアラートが出されます。

目的

これらの調査において問題を解決する上での組織の目的は、以下のとおりです。

- ユーザーの ID を判別する。
- 無許可のアクティビティーを目的として、誰が、または何が、その ID を使用しているのかを特定する。
- アクセス権限の誤用の目的を把握する。
- 同様に誤用される可能性のある ID を、該当のエンティティーが他にも持っているかどうかを評価する。

調査

「**Forensics**」タブのツールを使用して、調査に役立てます。

1. フリー・フォーム検索を使用して、機密システムやデータにアクセスしているアイデンティティーを検索します。
2. 疑わしいコンテンツを参照して、フリー・フォーム検索、データのピボット操作、およびコンテンツ・フィルタリングを行い、それらのアクセスの試みのいずれが疑わしいかを特定します。

3. アクセスされているコンテンツのデータの再構成を確認します。
4. Surveyor でアクセスのパターンを再トレースし、頻度を評価します。
5. デジタル・インプレッションを使用して、単一のエンティティーによって使用されている別名を明らかにします。

共謀

このシナリオでは、組織に対して、1 人以上の利害関係者が自分たちの間で、または外部の関係者と共謀して、組織に不利益となるアクティビティーを行っているというアラートが出されます。

目的

これらの調査において問題を解決する上での組織の目的は、以下のとおりです。

- 共謀しているエンティティーを判別する。
- 共謀者間の対話の性質とパターンを把握する。
- 計画の基になっているコンテンツを明らかにする。
- 計画の期間を明らかにして、リスクの範囲を把握する。

調査

「**Forensics**」タブのツールを使用して、調査に役立てます。

1. フリー・フォーム検索を使用して、関与しているエンティティーの ID を検索します。
2. 本製品によってフラグが立てられている疑わしいコンテンツを検査します。
3. デジタル・インプレッション、可視化、およびコンテンツ・フィルタリングを使用して、疑わしい関係を特定します。
4. Surveyor を使用して、関与しているエンティティーのアクティビティーをトレースし、対話の内容を取得します。
5. 再構成された文書を調べて、共謀の動機付けを明らかにします。
6. フリー・フォーム検索とデータのピボット操作を使用して、共謀アクティビティーの発端を見つけます。

システム破壊

このシナリオでは、組織に対して、1 人以上の利害関係者が運用を妨害しようとしているというアラートが出されます。利害関係者はプロキシーとして利用されている場合もあります。

目的

これらの調査において問題を解決する上での組織の目的は、以下のとおりです。

- システム破壊実行者を特定する。
- システム破壊実行者が使用した手法を把握する。
- 妨害の影響と範囲を評価する。
- システム破壊実行者がエクスプロイトした脆弱性を特定する。

調査

「**Forensics**」タブのツールを使用して、調査に役立てます。

1. フリー・フォーム検索を使用して、システム破壊の症状を検索します。
2. 本製品によってフラグが立てられている疑わしいコンテンツを検査します。
3. ビジュアル・ナビゲーション、デジタル・インプレッション、およびコンテンツ・フィルタリングを使用して、症状を調べ、システム破壊実行者の ID を検出します。
4. Surveyor を使用して、システム破壊実行者のアクティビティーをトレースします。
5. データの再構成を使用して、システム破壊実行者の役割と動機付けを明らかにします。
6. データの再構成を使用して、システム破壊実行者が使用したコンテンツを確認します。
7. フリー・フォーム検索、Surveyor、および疑わしいコンテンツを使用して、危殆化したシステムと、システム破壊を可能にした手順を明らかにします。

不正および濫用の調査

QRadar Incident Forensics を使用して、無許可トランザクション、リソースの未許可の割り振り、プロトコル逸脱、およびの法的規制の回避を見つけます。

無許可トランザクション

このシナリオでは、組織に対して、無許可トランザクションの結果として、事業運営に財政的な悪影響が出ているというアラートが出されます。

目的

これらの調査において問題を解決する上での組織の目的は、以下のとおりです。

- 無許可トランザクションを見つける。
- 無許可トランザクションに関与し、その責任を担うエンティティーを特定する。
- 無許可トランザクションの頻度と傾向を把握する。
- 無許可トランザクションのリスクの範囲を評価する。

調査

「**Forensics**」タブのツールを使用して、調査に役立てます。

1. フリー・フォーム検索を使用して、矛盾するトランザクションや疑わしいトランザクションを検索します。
2. フリー・フォーム検索とデータのピボット操作を使用して、これらのトランザクションの反復を検索します。
3. データのピボット操作とデジタル・インプレッションを使用して、疑わしいトランザクションに関連するエンティティーを検出します。
4. トランザクションのコンテンツを明らかにし、再構築された文書を確認することで、定量値を確認します。

リソースの未許可の割り振り

このシナリオでは、リソースの未許可の割り振りがあり、事業運営に財政的な悪影響が出る可能性があるという疑いを組織が持っています。

目的

これらの調査において問題を解決する上での組織の目的は、以下のとおりです。

- リソースの不適切な割り振りを見つける。
- リソースの不適切な割り振りに関与し、それに責任を有するエンティティーを特定する。
- リソースの未許可の割り振りの動機付けを把握する。
- 不適切に割り振られたリソースのサイズと範囲を評価する。

調査

「**Forensics**」タブのツールを使用して、調査に役立てます。

1. 割り振られたリソースに関連した通信には、フリー・フォーム検索を使用します。
2. フリー・フォーム検索、データのピボット操作、およびデジタル・インプレッションを使用して、リソースの未許可の割り振りを行っているエンティティーの ID を特定します。
3. 再構成された文書を確認し、可視化を使用することにより、関連した対話の内容を処理し、動機を評価します。
4. Surveyor を使用して、割り振りアクティビティーを再トレースし、不適切に割り振られたリソースの量を把握します。

プロトコル逸脱および法的規制の回避

このシナリオでは、組織に対して、ビジネス、IT プロトコル、および法的規制が回避されており、財政的な悪影響が出る可能性があるというアラートが出されます。

目的

これらの調査において問題を解決する上での組織の目的は、以下のとおりです。

- どのプロトコルまたは法的規制が回避されたかを評価する。
- この振る舞いに関与したエンティティーを特定する。
- これらのエンティティーの動機付けを把握する。
- この不正行為の広汎性を評価する。

調査

「**Forensics**」タブのツールを使用して、調査に役立てます。

1. フリー・フォーム検索を使用して、プロトコルまたはコントロールによって管理されているビジネス・プロセスを検索します。
2. フリー・フォーム検索、データのピボット操作、およびデータの再構成を使用して、プロトコルおよび法的規制の概要を示す文書との相互参照を行います。

3. コンテンツ・フィルタリング、フリー・フォーム検索を使用して、プロトコルや規制が回避された具体的なインスタンスを検出します。
4. デジタル・インプレッション、可視化、データのピボット操作、およびコンテンツ・フィルタリングを使用して、関連するエンティティーの ID を見つけます。
5. Surveyor を使用して、エンティティーのアクティビティーを再トレースし、考えられる動機付けを調べます。

証拠収集の調査

QRadar Incident Forensics を使用して、組織内の脆弱性のリスクを評価し、脅威または加害者の特定における信頼性を定量化して、セキュリティー対策を改善します。

脅威の特定における信頼性

このシナリオでは、組織に対して、特定の脅威、エクスプロイト、または脆弱性に関するアラートが出されます。通常の業務処理に優先する可能性がある修復作業を正当化するために、関連するすべてのリスクについての信頼区間を定量化する必要があります。

目的

これらの調査において問題を解決する上での組織の目的は、以下のとおりです。

- セキュリティー・リスクに対する感受性を検証する。
- セキュリティー・リスクの証拠があるかどうかを判別する。
- セキュリティー・リスクの広がりと金銭的影響を評価する。
- セキュリティー・リスクの性質を把握する。

調査

「**Forensics**」タブのツールを使用して、調査に役立てます。

1. 潜在的ターゲットのエンティティーを開始点として使用することにより、フリー・フォーム検索、疑わしいコンテンツ、およびデータのピボット操作を使用して、脅威、エクスプロイト、または脆弱性を検索します。
2. フリー・フォーム検索とデータのピボット操作を使用して、オカレンスをまとめます。
3. フリー・フォーム検索を使用して、影響について言及している可能性のある文書を相互参照します。
4. デジタル・インプレッションと可視化を使用して、影響を受けたエンティティーを特定します。
5. Surveyor を使用して、脅威または加害者に関連したアクティビティーを分析します。

セキュリティー対策の改善

新しい振る舞いおよび危険な振る舞いの検出は、既存のセキュリティー対策が十分であるかどうかを組織が評価する動機付けとなります。このシナリオでは、組織は、直面するリスクに対する組織のセキュリティー・ルールの有効性を確認しようとします。

目的

これらの調査において問題を解決する上での組織の目的は、以下のとおりです。

- 新しい振る舞いまたは危険な振る舞いを認識する。
- 既存のセキュリティー・ルールの有効性を評価する。
- 動的操作により明らかになるセキュリティー・ギャップを把握する。
- 提案されたセキュリティー対策の有効性を評価する。

調査

「**Forensics**」タブのツールを使用して、調査に役立てます。

1. フリー・フォーム検索を使用し、ドメインおよび組織の知識を使用することにより、モバイル・ユーザーやクラウド・ベース・サービスなどの、新しい振る舞いまたは危険な振る舞いを検索します。
2. 疑わしいコンテンツを調べ、Surveyor を使用して、これらの振る舞いと既存のセキュリティー・ルールまたはセキュリティー対策を相互参照します。
3. フリー・フォーム検索、Surveyor、コンテンツ再構成、および可視化を使用して、頻度またはフォールス・ポジティブに対するセキュリティー・ルールからのアラートを分析します。
4. フリー・フォーム検索、Surveyor、コンテンツ再構成、データのピボット操作、および可視化を使用して、既存のセキュリティー・ルールまたはセキュリティー対策では検出されていないフォールス・ネガティブを検出します。

リスク・アセスメント

このシナリオでは、特定の脆弱性、エクスプロイト、または悪意のある振る舞いの概要を示すセキュリティー情報により、組織は、リスク・アセスメントを行うように促されます。リスク・アセスメントにより、組織が影響を受けやすいか、あるいは既に危殆化しているかを判別します。

目的

これらの調査において問題を解決する上での組織の目的は、以下のとおりです。

- 特定された脆弱性の組織内での存在を評価する。
- 外部の関係者について、悪意のある存在を検出する。
- 危殆化の証拠を明らかにする。
- 組織がエクスプロイトの被害者であるかどうかを判別する。
- ユーザーの ID を判別する。

調査

「**Forensics**」タブのツールを使用して、調査に役立てます。

1. フリー・フォーム検索を使用して、セキュリティー情報で指定された脆弱性、エクスプロイト、または他の悪意のある振る舞いの特徴を検索します。
2. フリー・フォーム検索を使用して、調査または他のデータを相互参照し、指標を導き出します。

3. Surveyor を使用して、特定された脆弱性をエクスプロイトした可能性のある対話を調査します。
4. 本製品によってフラグが立てられている疑わしいコンテンツを検査します。
5. データの再構成を使用して、潜在的に危険な対話の基となるコンテンツを確認します。
6. Surveyor を使用して、潜在的に危険なエンティティーのアクティビティーを再トレースします。

第 3 章 Forensics 調査の開始

IBM Security QRadar Incident Forensicsで Forensics 調査を開始するには、「**クイック・スタート (Quick Start)**」メニューを使用して、Forensics リポジトリーにあるデータのナビゲートとフィルタリングを行います。このランチパッドには、事前定義されたサマリー照会が含まれています。これを使用して、検索を開始したり、エンティティーの関係を取得したりすることができます。

開始時には、以下のガイドラインに従ってください。

1. 「**オフェンス**」タブで、オフェンスから Forensics リカバリーまたは Forensics 検索を開始します。
   - オフェンスまたは任意の IP アドレスを右クリックして Forensics リカバリーを実行すると、Forensics は指定された時刻範囲の生のキャプチャー・データをキャプチャー・デバイスから取得し、文書を抽出および再作成した後、結果を Forensics リポジトリーに追加します。
   - オフェンスまたは任意の IP アドレスを右クリックして Forensics 検索を実行すると、Forensics リポジトリーがフィルターに掛けられ、その IP アドレスが検索されます。その後、「**Foresnics**」タブのメイングリッドに結果が表示されます。照会を作成すると、検索を詳細化できます。

   QRadar Incident Forensics は検索要求を受け取ると、パケット・キャプチャー・データを処理し、対象受信者に送信されたフォーマットにそのデータを戻します。例えば、Microsoft Word 文書は Word ファイルとしてリカバリーされます。Voice-over-IP 通話は音声ファイルとしてリカバリーされます。その後、リカバリーされたファイルを検索可能な状態にするために、メタデータとファイル内容の両方を使用してファイルの索引付けが行われます。
2. 「**Forensics**」タブで、「**クイック・スタート (Quick Start)**」をクリックします。

   リカバリーまたは検索を実行したら、フリー・フォーム検索を行って独自の照会を作成するのではなく、「**Forensics**」タブの「**クイック・スタート (Quick Start)**」メニューから事前定義された照会を使用することで、すぐに調査を開始できます。例えば、「**疑わしいコンテンツ (Suspect Content)**」カテゴリーを参照し、「**エンティティー・アラート (entity alert)**」など、いずれかの照会を実行することができます。*疑わしいコンテンツ* とは、疑わしいアクティビティーの前兆となるコンテンツについて定義されたルール・セットに基づきます。*エンティティー・アラート* は、セキュリティー・ポリシー違反に関わる、悪意のある可能性があるエンティティーにフラグを立てます。

   コンテンツのカテゴリー化とフィルタリング機能は、返されるデータの量を減らすのに役立ちます。
3. 「**グリッド (Grid)**」から、調べる文書を選択します。

QRadar Incident Forensics により、優先順位付けされた検索結果が返されます。インターネット検索で検索エンジンの最適化によってサイトが優先順位付けされるのと同じように、最も頻度の高いオカレンスがリストの先頭に表示されます。

データのピボットを開始するには、リンクをクリックし、文書に関連付けられたメタデータを検索します。データ・ピボット機能には、さまざまな検索ビューとデータ・サマリーが用意されています。

4. すべてのアクションとセキュリティー・インシデントの間の関係を調査するには、文書ビューでリンクを選択し、「**次の関係を取得 (Get relations for)**」を右クリックします。

   属性を調査したら、エンティティーを接続することで収集した情報をフィルターに掛けます。

5. 「**デジタル・インプレッション (Digital Impressions)**」をクリックし、アイデンティティー証跡を辿って、コンパイルされた関連付けセットを取得します。

   デジタル・インプレッションはメタデータの索引です。これは、悪意のあるユーザー証跡を辿って、攻撃者や不正内部者の疑いのあるユーザーを特定するのに役立ちます。これらの関係を構築する際に、QRadar Incident Forensics は IP アドレス、MAC アドレス、TCP ポート、TCP プロトコルなどのネットワーク・ソースからのデータを使用します。チャット ID などの情報を検出したり、ワード・プロセッサー・アプリケーションやスプレッドシート・アプリケーションから作成者 ID などの情報を読み取ったりすることができます。デジタル・インプレッションは、エンティティーのアイデンティティーを他のユーザーまたはエンティティーの識別情報とリンクすることで関連付けを見つけるのに役立ちます。

QRadar Incident Forensics の検索とブックマーク

調査担当者は IBM Security QRadar Incident Forensics を使用して、ネットワーク・トラフィックや文書から関連データを抽出します。

レコードの検索およびブックマーク

直観的なフォレンジック・アクティビティーを可能にするために、QRadar Incident Forensics では、パケット・データを取得し、他のコンテンツを取り込みます。このテクノロジーは、検索主導型のデータ探索、セッションの再構成、およびフォレンジック・インテリジェンスを提供し、セキュリティー・インシデントの調査を支援します。

調査担当者は、大まかな操作で調査の焦点を絞り込んだ後、その結果を微調整して、関連のある最終的な結果セットを導き出します。簡単でハイレベルなアプローチでは、最初に多数のレコードを検索してブックマークを付けます。次に、ブックマークを付けたレコードに焦点を当てて、最終的なレコードのセットを特定します。関係のある情報を判別し、照会を微調整して、項目を含めたり、除外したりします。その情報を使用して、仮説を証明します。

新しい手掛かりが明らかになったら、他の方法を使用してそれらの手掛かりを追跡調査できます。視覚化ツールと分析ツールを使用して、手動または自動で結果の関連性を評価できます。さらに、各種の照会を使用して、同じ問題の別の側面を取り出すこともできます。

ブックマークの付いた結果の処理

調査にとって重大な結果を得たら、その結果にブックマークを付けて、詳しい検査や最終的な決定に備えておくことができます。ブックマークは、必要と思う以上に行ってください。疑わしい場合は、ブックマークを付けてください。その上で、無関係な情報を除去し、関係すると思う情報に焦点を合わせてください。

関係すると思う一連の結果にブックマークを付けた後、検査を微調整することができます。

1. 視覚化ツールおよび分析ツールを使用して、ブックマークを付けたそれぞれの文書を調べます。
2. ケースのメモを文書に追加し、ケースとの関連性の観点から各文書に最終的な判断を下します。
3. レコードが無関係な場合は、そのブックマークを削除します。

   調査過程で、リポジトリーにある関連情報を特定し、関連するレコード群にブックマークを付けた状態になっています。
4. 関連するレコードを印刷、エクスポートまたは処理します。

文書の検索と調査

調査担当者は、セキュリティー・インシデントがどのように発生したかの手掛かりや仮説に関連した文書を検索します。

検索

大量の文書を手作業で取捨選択しようとしても、ほとんどの文書はケースに無関係です。代わりに、調査担当者は Forensic リポジトリーを使用して、着目している特性を満たす文書を抽出します。例えば、特定の期間内に発生した文書は、着目しているトピック、つまり攻撃者が送受信した文書に関連します。

具体的に検索できます。具体的な検索の例としては、「文字ストリング “Mission Alpha” の完全一致の検索」があります。あるいは、汎用的な検索もできます。より汎用的な検索の例としては、「リポジトリー内にあるすべての社会保障番号の検索」があります。

1 つの条件にのみ基づいて、単純な検索を行うことができます。複雑な検索の結果は、複数の条件を満たすものでなければなりません。複雑な検索では、例えば、あるトピックについて 2 人の攻撃の容疑者の間で交わされたすべての E メールを検索し、このうち、添付ファイルを含む E メールを除外します。検索の目的は、扱いやすい作業セットになるまで、レコードを迅速かつ正確に絞り込むことです。調査担当者が検査する文書セットの規模が小さいほど、文書とケースとの関連度がより高くなります。

IP アドレスまたはポートのリカバリーの実行

1 つ以上の IP アドレスまたは 1 つ以上のポートのリカバリーを実行できます。IP アドレスおよびポートを入力しないと、すべての TCP トラフィックおよび UDP トラフィックがリカバリーされます。複数の IP アドレスやポートを入力する場合、これらを区切るためにコンマを使用する必要があります。

制約事項: 原則として、一度に約 7 つの IPv4 アドレスと 7 つのポート、または最大約 255 文字を入力できます。「**IP アドレス**」フィールドおよび「**ポート**」フィールドと他の語句が結合され、フィルター・ストリングが作成されます。フィルター・ストリングは 255 文字を超えないようにしてください。

Forensic のケース

ケースとは、インポートした文書およびパケット・キャプチャー・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。

ケースを作成するのは、管理者か、ケース作成の特権を持つ調査担当者のいずれかです。管理者は、ケースを作成して調査担当者に割り当てます。調査担当者は、IBM Security QRadar で IP アドレスからパケット・キャプチャー・データを取得するときに、新しいケースを作成できます。

関連タスク:

17 ページの『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アップロード』
外部データを特定のケースにアップロードすることができます。

コレクション

パケット・キャプチャー (pcap) データ・ファイル、PDF、またはネットワーク・ストリームなどの、特定のソースから得た関連データをグループ化するには、コレクションを使用します。

コレクションは、関連データのグループを明確にして管理するために使用します。調査が完了したら、コレクションにあるグループ・データを簡単に削除することができます。

コレクションを作成するのは管理者または調査担当者です。管理者はコレクションを作成し、手動でデータを IBM Security QRadar Incident Forensics にロードします。管理者もコレクションをケースに追加します。調査担当者は、IBM Security QRadar で IP アドレスからのパケット・キャプチャー・データの取得を開始するときに、新しいコレクションを作成することができます。

コレクションおよびコレクション名については以下の規則を念頭に置いてください。

- コレクション名は固有でなければなりません。
- ケースには 1 つ以上のコレクションを含めます。
- コレクションは複数のケースに追加することができます。
- 同じコレクションを含む 2 つのケースを調査担当者が所有している場合は、重複するデータが検索結果に返されます。
- コレクション名が固有でない場合は、新しい pcap をアップロードすると、元のコレクションが削除された上で新しい pcap がアップロードされます。

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アップロード

外部データを特定のケースにアップロードすることができます。

始める前に

管理者は、外部ファイルをアップロードするユーザーに対して、セキュア FTP 許可を有効に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、ネットワーク上の任意のアクセス可能なディレクトリーからデータをインポートできます。データは、以下を始めとする、多数の形式がサポートされます。

- 外部ソースからの標準的な PCAP 形式のファイル
- テキスト・ファイル、PDF ファイル、スプレッドシート、および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

複数のファイルをケースにアップロードできます。

制約事項: ケース名は固有でなければなりません。既存のケースと同じ名前を持つケースを作成することはできません。

手順

1. FTP クライアントで、以下のステップを実行します。
   a. トランスポート層セキュリティー (TLS) がプロトコルとして選択されていることを確認してください。
   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 の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。
2. QRadar Incident Forensics サーバーに接続し、新規ディレクトリーを作成します。
3. FTP で PCAP ファイルを転送し、保管するには、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、PCAP ファイルをそのディレクトリーにドラッグします。
4. FTP で PCAP ファイル以外の他のファイル・タイプを転送し、保管するには、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、ファイルをそのディレクトリーにドラッグします。
5. 以下のコマンドを入力して、FTP サーバーを再始動します。

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

6. 以下のコマンドを入力して、アップロード領域から QRadar Incident Forensics ディレクトリーにファイルを移動するサーバーを再始動します: service decapper restart

タスクの結果

「**Forensics**」タブ上のいずれかのツールに、ケースが表示されます。

Forensics リポジトリーの照会

調査担当者は、Forensics データベースから取得したいと思っている文書の特性を指定します。複数の照会を使用して、調査する文書群を検索します。

少量の文書群に対して複数の照会および手動での検査を行うほうが、リポジトリー全体から取捨選択するより優れています。多くの場合、その後の照会や詳細な照会に対するアイデアは、無関係な文書の検査中に生まれるものです。

照会語の数を増やしたり限定性を強くしたりすると、関連性の高い結果セットが得られます。目標は、必要な結果に関して知っている限りの情報を定義すること、および可能であれば厳密にすることです。検索条件には、任意の数の照会語を入力することができます。照会語はスペースまたはブール演算子で区切ります。スペースのみで区切った検索語は、暗黙的に論理 OR のブール演算子を示します。OR 演算子は、いずれかの検索語が検出されれば、どの検索語であっても同等の価値があることを意味します。最も多くの検索語を満たす結果がリストの一番上に置かれ、照会語に対する一致度の高さを示します。

単一の検索条件を照会語ともいいます。通常、検索には複数の照会語が含まれます。1 つの検索に対する照会語の集合を照会ストリングともいいます。照会の式を組み立てるのに精通するには練習が必要ですが、難しくはありません。いくつかの照会語と、組み合わせで必要な条件を作成したり否定したりする方法を学習することだけです。照会ストリングは QRadar Incident Forensics に保存されるため、データに関する知識が増えるに従って継続的に検索を微調整することができます。

関連タスク:

30 ページの『関係の視覚化』
復元した文書の属性間の関係を参照するには、 「視覚化 (Visualize)」ウィンドウを使用します。例えば、特定の E メール・アドレスと通信した E メール・アドレスを調べることができます。

フリー・フォームの照会語

調査担当者が文字ストリングに完全に一致するものを検索するには、「**Forensics**」タブの検索条件フィールドに照会語を直接入力します。1 つの単語または複数の単語による照会を使用することができます。

使用できる検索照会の種類について以下の表で説明します。

表 1. フリー・フォーム照会の種類

検索照会の種類	説明	例
1 単語の照会	文書の中で 1 つの用語を検索します。	puppies
ワイルドカードを含む 1 単語の照会	照会語の中間または末尾で 1 つ以上の文字に一致するものを検索します。 **制約事項:** ワイルドカード文字を検索の先頭文字として使用することはできません。	te?t test* te*t

表 1. フリー・フォーム照会の種類 (続き)

検索照会の種類	説明	例
複数単語の照会	照会語の関連性の順位に従って検索結果を返すように指定します。両方の照会語を含む文書が最初にリストされ、一方の照会語しか含まない文書がその後にリストされます。照会語を 1 つしか含まない文書には、個々の照会語の出現数に応じた順位が付けられます。	free puppies
二重引用符付きの複数単語の照会	正確な文字列で突き合せます。両方の単語を含むが、順序と隣接関係がこのとおりでない文書は結果として返されません。実質的に、二重引用符によってこれら 2 つの単語が 1 つの文字列や 1 つの照会語になります。検索エンジンから見ると、2 つの別々の単語ではなくなっています。	"free puppies"
AND 演算子を使用する複数単語の照会	両方の照会語が文書に存在しなければ一致と見なさないことを指定します。照会語の順序は任意であり、必ずしも相互に近接していなくても構いません。	free AND puppies

メタデータ・タグ

共通するエンティティーにはタグが付けられるため、調査担当者は、関連した文書から正確な結果セットを迅速に得ることができます。

Incident Forensic 索引では、セッション、文書、またはプロトコルの種類に応じて多くのメタデータ・フィールドが使用される場合があります。

メタデータ・タグ名を指定するときには、Forensic リポジトリーに存在するものを正確に指定しなければなりません。

メタデータ・タグ検索の種類を以下の表に示します。

表 2. メタデータ・タグ検索

メタデータ・タグ検索の種類	形式	例
標準	`MetadataTag:<value>`	`ApplicationProtocol:http`
ワイルドカード	`MetadataTag:*`	`CreditCardNumber:*`
範囲	`MetadataTag:[<start value> TO <end value>`	`Duration:[30 TO 56]`

関連概念:

23 ページの『文書の注釈』
調査担当者は、ケース内の文書に関する考えや説明を追跡するために、文書にブックマークを付けたり文書にメモを追加したりします。

ブール結合

複数の照会語を、簡単なブール演算子を使用して繋ぎ合わせて、対象を詳細に指定する照会ストリングを作成することができます。照会ストリングを適切に作成すると、調査担当者が探しているものに厳密に一致する結果を得ることができます。

基本的なブール演算子は AND、OR、NOT、および () です。AND 演算子は、文書の中で両方の照会語が一致しなければならないことを指定します。OR 演算子は、文書の中でいずれかの照会語を検出できることを指定します。NOT 演算子は、否定される照会語に一致する結果を否定 (除外) します。() 演算子は、照会語および値をグループ化してその集合に関数を適用したり、複数の値を 1 つの関数に適用したり、構文を明確化したりします。

ブール演算子は大文字にする必要があります。

ブール演算子と照会ストリングの例を以下の表に示します。

表 3. 照会ストリングに対するブール演算子

ブール演算子	照会ストリングの例	例の説明
AND	`TcpPort:80 AND Protocol:http`	2 つの照会語を使用して、標準的な Web トラフィックをすべて検索します。Web テストをポート 8080 で行う場合は、両方の照会語が真にならないため、一致しません。
OR	`Collection:yahoo* OR Collection:cnn* OR Collection:msn*`	3 つの照会語を使用して、結果を、Forensics リポジトリーにある Yahoo、CNN、および MSN の文書コレクションからの結果に制限します。
NOT	`ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080 OR 81)`	標準的でない方法でポートを使用したトラフィックを検索します。最初の照会語は、標準的な HTTP トラフィックを検索します。2 番目の照会語は、HTTP を受け付けるポートを使用しているすべてのトラフィックを除外します。

()	`(ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080)) OR (ApplicationProtocol:pop* AND NOT ServerTcpPort:110)`
	
	`NOT (Collection:yahoo* OR Collection:cnn* OR Collection:msn*)`
		これらの照会では、括弧を効果的に使用して複雑な条件を実現しています。括弧がなければ、これらの照会はさらに長く複雑になり、定式化やデバッグがしにくくなります。

照会ビルダー・ツール

検索を作成したり保存済み検索を管理したりするには、照会ビルダー・ツールを使用します。

照会ビルダー・ツールは、調査担当者に、強力な検索を作成するプロセスをグラフィカルに経験させます。強力な検索は、照会語が例とともに分類されたリストを使用します。

表 4. 照会ビルダー・ツールのパラメーター

パラメーター	説明
カテゴリーの選択	「**フィールドの選択**」リストで使用可能なメタデータ・タグのリストをフィルターに掛けます。
フィールドの選択	Forensic リポジトリーで情報へのタグ付けに使用するメタデータ・タグ。
照会の例	「**照会の入力 (Query Input)**」フィールドにある照会を実行し、結果の件数を報告します。
新規	「**照会の挿入 (Insert Query)**」をクリックしたときに、既存の照会を新しい照会で置き換えます。
AND	「**照会の挿入 (Insert Query)**」をクリックしたときに、新しい照会を既存の照会と結合します。文書は両方の照会語に一致しなければなりません。
OR	「**照会の挿入 (Insert Query)**」をクリックしたときに、新しい照会を既存の照会と結合します。文書はいずれかの照会語に一致しなければなりません。

調査担当者は、ファイル・システムのフォルダーに検索を保存して整理することができます。これにより、調査担当者同士での共有が可能になります。調査担当者は、保存済み照会の説明や名前を、参照用、管理用、および目的の把握のために使用します。

「**照会 (Query)**」タブの「**照会の使用 (Use Query)**」機能は、保存済みの照会を実行するために「**検索条件の入力 (Search Criteria Input)**」フィールドに送信する目的で使用されます。

以前に実行された照会を調査担当者が探して再実行するには、以前の照会リストを使用し、実行したい照会を選択して「**照会の挿入 (Insert Query)**」をクリックします。

照会フィルター・ツール

照会フィルター・ツールは、アクティブ・データを使用して、永続的フィルターを作成するための視覚的な手掛かりを提供します。

照会フィルターは、永続的なバックグラウンド・フィルターであり、照会ストリングによる問い合わせが行われているアクティブな文書セットを削減します。フィルターを使用することにより、照会ストリングに静的な照会語を詰め込みすぎることなく、使用可能な文書セットが削減されます。結果として、照会ストリングをより細かく制御できます。

照会フィルターは、ケース依存のフィルター・タイプ・リスト、動的更新、およびリアルタイムでの結果サマリーをサポートするため、調査の手始めに使用するのに適しています。フィルター・タイプ・リストには、使用可能なケース内で検出されたすべての値が取り込まれます。所有するケース内にどのようなデータが含まれているかを素早く確認できます。フィルター・タイプ・リストの項目を選択したりクリアしたりすると、結果サマリーが自動的に更新されます。フィルターの有効性や、フィルターを適用した状態でどのくらいの量の文書セットが残っているかが、すぐにわかります。

デフォルトの照会フィルターのチューニングは、再利用する照会の場合はお勧めしません。照会を保持したい場合は、新しい照会フィルターを作成してください。デフォルトの照会フィルターを変更した場合は、終わった時点でリセットし、その後の検索照会で文書が誤って除外されることがないようにしてください。

アクティブ・フィルターの結果

調査担当者は、照会フィルター・ツールの結果サマリー・セクションでアクティブ・フィルターからの結果を表示します。

フィルターが変更されるとサマリーも更新され、総文書数および使用可能な文書の数が表示されます。総文書数は、調査担当者が使用可能であるフィルター適用前の文書数です。使用可能な文書数は、フィルター適用後に使用可能な文書の数です。調査担当者は、これらの数を使用してフィルターの有効性を判断し、フィルター作成時に適宜調整します。

照会フィルター・ツールの検索フィルター

調査担当者はデータをフィルターに掛けて、割り当てられたケースを検索します。データは、フィルター・タイプ (IP アドレスや MAC アドレスなど) によってグループに分類されます。

調査担当者は、ロジック・アクションの切り替えを使用することで、リストから選択した項目を含めるか除外することができます。

各検索フィルター・グループにはロジック・アクションの切り替えが備わっており、リストで選択した項目を含めるか除外するように設定できます。含めるように設定すると、リストの項目が論理 AND で結合され、選択したすべての項目を含む使用可能な各文書が選択されます。除外するように設定すると、論理 OR が使用され、選択した項目をいずれも含まない使用可能な各文書が選択されます。

調査担当者は、**UserQuery** グループを使用して、独自の照会ストリングを定式化し、フィルターに追加することができます。

検索で返される文書数の制限

IBM Security QRadar Incident Forensics の照会にフィルターを追加して、検索結果ページに表示される文書の数やタイプを制限することができます。

手順

1. 「**Forensics**」タブで、「**照会フィルター (Query Filters)**」アイコンをクリックします。

   データがフィルター・タイプ別のグループに分けられます。

2. 「検索フィルター (Search Filters)」ウィンドウで、フィルター・タイプごとに「**含める**」または「**除外**」をクリックして、検索結果に文書を含めるかどうかを選択します。
3. フィルター・グループ内の項目を見つけるには、以下の手順を実行します。
   a. 「**フィルター・タイプ (Filter Type)**」列で、フィルター・グループを展開します。
   b. 「検索」ウィンドウで、基準を選択して「**検索 (Find)**」をクリックします。

   「**Web カテゴリー (Webcategory)**」フィルター・グループでレコードを検索すると、一致するカテゴリー・フィールドがすべて表示されます。例えば、「**Web カテゴリー (Webcategory)**」「**等しい**」「**チャット**」を検索すると、「**チャット**」と関連カテゴリー (「**インスタント・メッセージング (Instant Messaging)**」、「**Web メール/ユニファイド・メッセージング (Webmail/Unified Messaging)**」、「**検索エンジン/Web カタログ/ポータル (Search Engines/Web catalogs/Portals)**」、「**クラウド**」など) が表示されます。

文書の注釈

調査担当者は、ケース内の文書に関する考えや説明を追跡するために、文書にブックマークを付けたり文書にメモを追加したりします。

文書へのブックマーク追加は、メインの結果画面のほか、対話中に交換される一連の文書を表示する日時順グリッド上の Surveyor ツールで行うことができます。照会や調査は複雑になる場合があるため、調査担当者は、関心の低い文書も含めてすべてのレコードにブックマークを付けます。ブックマークを使用すると、複雑な照会を再作成したり一連の調査をたどり直したりする必要がなくなります。注釈は、レコードにブックマークを付けた後に作成することができます。

調査中に、複数のパスをたどりたい状況になることがあります。ブラウザーの機能を使用して、現在操作しているタブを複製します。タブを複製することにより、戻って別のパスをたどることを覚えておく必要も、分岐点に至る過程を覚えておく必要もなくなります。現在のタブは、必要に応じて何回でも複製することができます。それぞれのパスを別のタブでたどり、その過程で関連文書にブックマークを付けます。ブックマークを付けた各文書に至るパスを明示するメモを追加することができます。

メモは、調査中に考えたことを記録する手段です。メモを削除できるのは管理者のみです。メモには、調査担当者のユーザー ID と入力時のタイム・スタンプがタグとして付けられます。文書をエクスポートすると、再構成された文書およびその属性とともにメモが出力されます。

関連概念:

19 ページの『メタデータ・タグ』
共通するエンティティーにはタグが付けられるため、調査担当者は、関連した文書から正確な結果セットを迅速に得ることができます。

第 4 章 調査ツール

調査担当者は、Surveyor ツール、デジタル・インプレッション・ツール、エクスポート・ツール、および視覚化ツールを使用して、さまざまな方法でデータを管理します。

「検索結果」ページは「**Forensics**」タブのデフォルト・ページです。検索結果は「**グリッド (Grid)**」タブで参照できます。調査担当者は、グリッドの検索結果を使用して、迅速に文書の検索やアクセスを行えます。「**グリッド (Grid)**」タブでは、Surveyor ツール、デジタル・インプレッション・ツール、エクスポート・ツール、および視覚化ツールを使用して詳細な調査を行います。

行インディケーター

行インディケーターにより、結果セットに返された各文書に固有の ID が割り当てられます。行インディケーターは、文書および必要なすべての関連文書を「再構成ビュー (Reconstructed View)」視覚化ツールに送信するために使用します。

行のソート

グリッドに表示されている行をソートすることができます。グリッドに表示されている結果の数よりも結果の総数が多い場合があるため、結果セット全体をソートすることはできません。

文書閲覧済みインディケーター

文書閲覧済みインディケーターは小さい円であり、赤と緑の間で切り替わって、調査担当者が文書を表示したかどうかを示します。

文書の選択

調査担当者は、表示対象文書のセレクターを使用して、結果グリッドに表示する文書の数を選択します。「すべて選択」を使用すると、後続の機能に文書を送信することができ、処理または視覚化のために多数の文書を送信できます。表示対象文書のセレクターを使用して文書を選択すると、グリッドに表示されている文書だけでなく、すべての文書を選択することになります。

ネットワークと文書の視覚化

調査担当者は、パターンを検出したり、指定した期間に最も多くのネットワーク・トラフィックや文書の輻輳 (ふくそう) が発生した個所を把握したり、疑わしいコンテンツを表示したりするために、視覚化ツールを使用します。例えば、調査担当者はネットワーク・トラフィックのパターン (企業の終業後にアクセスされたサーバーなど) を視覚化することができます。

VGrid ツールは時間ブロックに分割されます。グリッドでは、疑わしいコンテンツ (ネットワーク・トラフィックや文書など) が赤い長方形で示されます。緑色の長方形は通常のコンテンツを示します。明るい色のブロックはトラフィックが多いこと

を示します。色の彩度が高いほどトラフィックの量が多いことを意味します。時間ブロックの明るさは、VGrid ツールに表示されている現在のデータに相関しています。例えば、ある時間ブロックの色が明るくても、それよりもデータが多い別の時間ブロックがロードされると、色が暗くなります。

調査担当者は、コンテンツを含む各時間ブロックでのネットワーク・トラフィックの種類および文書の数を表示することができます。

時間ブロック内のネットワーク・トラフィックと文書の検査

調査担当者は、特定の時間ブロック内の、個々の文書、表示された Web サイト、または送信メールを検査することができます。

手順

1. 「**Forensics**」タブで「**VGrid**」タブを選択します。
2. 以下のいずれかのオプションを使用して、時間ブロック内のコンテンツを検査します。
   - ネットワーク・トラフィックの種類および文書の数を表示するには、時間ブロックの上にマウス・ポインターを移動します。
   - 時間ブロック内のコンテンツを検索するには、1 つ以上の時間ブロックを選択します。右クリックをして 「**選択した時間ブロックの検索 (Search selected time blocks)**」を選択します。
   - 一連のイベントを表示するには、時間ブロックを選択してから「**Surveyor (Surveyor)**」を選択します。
   - コンテントを視覚化するには、時間ブロックを選択してから「**視覚化 (Visualize)**」を選択します。

Surveyor ツール

セキュリティー・インシデントにおける一連のイベントを発生順に視覚化するには、Surveyor ツールを使用します。

このツールは、攻撃者が表示した内容と操作を調べるために、調査担当者が使用します。Surveyor ツールにより、セキュリティー・インシデントでのアクティビティーが、動画プレイヤーのように日時順で表示されます。Surveyor は時間指向であるため、結果画面から 1 つの文書を選択しても情報はあまり表示されません。選択した文書が少なすぎる場合は、「**属性 (Attributes)**」タブで、選択した文書の前後の時刻範囲を拡大します。「**コンテキストの表示 (Show Context)**」リンクをクリックして、時間を拡大します。

調査担当者は、ケースの時刻、プロトコル、および IP アドレスによって照会をフィルターに掛けることができます。

「**リスト**」タブを表示すると、送受信された文書が日時順のリストで表示されます。Surveyor ツールでは、対話がステップバイステップで再現されます。

文書の ID 番号が緑色の場合は、調査担当者によって文書がレビューされたことを示します。ID 番号が赤い場合はレビューされていません。

再構成された文書の表示

「**表示 (View)**」タブには、「リスト」ビューの画面の左側で選択した文書の再構成されたものが表示されます。

左側での順序付けと右側での再構成の組み合わせは強力であり、攻撃者がネットワーク上で何を表示して何を行ったかを調べることができます。Surveyor は、ネットワークをトラバースした目に見える文書のほかに、裏で行われたコンピューター間のハンドシェークや証明書の交換も表示します。

関連タスク:

39 ページの『第 5 章 IP アドレスに対するネットワーク・トラフィックの調査』
セキュリティー・インシデント中に行われた会話での関連するコンテントを視覚化するために、IP アドレスに関連したネットワーク・トラフィックを復元して再構成することができます。IP アドレスに関連する既存のケースを検索することもできます。

抽出される文書の内容

「**テキスト**」タブには、文書から抽出された内容が表示されます。文書の内容は不定形式です。

このテキストは、検索エンジンのインデクサーから得られるものです。

QRadar Incident Forensics での文書のエクスポート

IBM Security QRadar Incident Forensics では、エクスポートされた PCAP 文書を除くすべてのエクスポート文書に、再構成された文書、文書の未加工テキスト、属性、および文書に添付されたメモが含まれます。

PCAP 文書のエクスポート時には、再構成は行われません。例えば、Web ページをエクスポートする際には、メイン接続中にブラウザーがダウンロードしたものがすべてダウンロードされます。通常、メイン接続中にはテキスト・コンテンツのほとんどがダウンロードされます。ただし、最新のブラウザーの大半は、より多くのアイテム (スタイル・シートやイメージなど) をダウンロードするために複数の接続を使用しており、これらはエクスポートには含まれません。エクスポート時には、PCAP コンテンツは最初に再構成されません。

別の例として、複合プロトコル (FTP や VOIP など) があります。このようなプロトコルでは、メインコマンドと制御接続のほかに、別個のデータ接続があります。VOIP 通話や FTP ダウンロード用の PCAP ファイルをエクスポートする場合は、データが再構成されず、予期しない結果になる可能性があります。

pcap ファイルとして文書をエクスポート

複数の IBM Security QRadar Incident Forensics および IBM Security QRadar Packet Capture のアプライアンスから pcap ファイルとして文書をエクスポートできます。

制約事項: pcap フォーマットにエクスポートするコンテンツは、再構成されません。

手順

1. 選択した文書からデータをエクスポートするには、「**Forensics**」タブの復元グリッドで、文書の横にあるチェック・ボックスを選択してから、「**エクスポート**」をクリックします。

   pcap フォーマットにエクスポートする文書は、最大 25 件まで選択できます。
2. 「**エクスポート・タイプの選択 (Select Export Type)**」リストから、「**PCAP**」をクリックします。
3. QRadar Incident Forensics ホストのすべての文書がエクスポートされたら、「**ダウンロード**」をクリックすることができます。
4. 文書のエクスポートが失敗した場合、**失敗**のメッセージをクリックして、文書を再度エクスポートします。

タスクの結果

1 つの pcap ファイルをエクスポートする場合は、その pcap ファイルがダウンロードされます。複数の pcap ファイルをエクスポートする場合は、それらの pcap ファイルが 1 つの圧縮ファイル (.zip) にまとめられ、この圧縮ファイルがダウンロードされます。

各文書には、QRadar Incident Forensics ホストの IP アドレスと、その文書の取得元である QRadar Packet Captureデバイスの IP アドレスが格納されます。QRadar Incident Forensics ホストを削除した場合、または QRadar Packet Capture を移動した場合、エクスポートを実行できない可能性があります。

デジタル・インプレッション

デジタル・インプレッション は、アイデンティティー証跡を識別する関係をまとめたものです。デジタル・インプレッションはネットワーク関係を再構成し、攻撃元エンティティーのアイデンティティー、通信方法、および通信相手を突き止めることを支援します。

以下のような重要な疑問に対する答えを迅速に得るには、デジタル・インプレッション・ツールを使用します。

- この疑わしい攻撃者、コンピューター、または IP アドレスについて何が分かっているか。
- この疑わしい攻撃者と対話したことがあるのは誰か。
- 疑わしい攻撃者が接触しているネットワーク内に誰がいるか。
- この攻撃者は、アイデンティティーを偽ろうとしているか。

オンライン ID

オンライン ID (E メール・アドレス、Skype アドレス、MAC アドレス、チャット ID、ソーシャル・メディアの ID、Twitter の ID など) は、エンティティーや個人の識別に使用されます。ネットワーク・トラフィックおよび文書で検出される既知のエンティティーや個人には自動的にタグが付けられます。

IBM Security QRadar Incident Forensics は、デジタル・インプレッションを生成するために、相互に対話したタグ付きの ID を相関させます。

デジタル・インプレッション・レポートのコレクション関係は、攻撃者、ネットワーク関連のエンティティー、またはデジタル・インプレッション・メタデータの用語に関連する、継続的に収集された電子的存在を表します。調査担当者は、文書に関連付けられた任意のタグ付きデジタル・インプレッション ID をクリックすることができます。得られるデジタル・インプレッション・レポートは表形式でリストされ、ID タイプごとに編成されています。

関係情報の取得

デジタル・インプレッション・レポートには、 *中心 ID* とそれ以外のすべての ID との間の対話が示されます。*中心 ID* とは、セキュリティー・インシデントにおいて着目の起点にするオンライン ID のことです。

通常、多くのカテゴリーで最上位を占める ID は、その ID タイプまたはカテゴリーにおける中心 ID のアイデンティティーです。例えば、ID が MAC アドレスである場合、最も対話が多い E メール・アドレスが、そのMAC アドレスのコンピューターを所有している疑わしい攻撃者に帰属している可能性があると考えられます。しかし、IP アドレスが動的に割り当てられる場合は、一定の時間範囲にわたって割り当てられていた IP アドレスも調査する必要があります。

通常は、他のカテゴリーと中心 ID の間の相関関係はあまり強くありません。デジタル・インプレッションに基づいて行動の決定を下す前に、複数の独立したソースでデータを検証してください。デジタル・インプレッション・ツールを使用して、さらなる疑わしい攻撃者やエンティティーに調査の範囲を広げてください。

関係の調査によるアイデンティティー証跡の追跡

デジタル・インプレッションはネットワーク関係を再構築して、攻撃しているエンティティーと、そのエンティティーが通信している他のエンティティーの特定を助けます。

デジタル・インプレッション・ツールには、相関イベントの頻度分布が表示されます。このツールは、エンティティー間の関係を表示し、関係をカウントします。カウントが増えると、関係がより強くなります。例えば、E メール・アドレスと他のエンティティーとの関係を見ると、誰が誰と通信しているかを把握できます。 E メール・アドレスに関連付けられている IP アドレス、疑わしいユーザーがアクセスした IP アドレス、およびその E メール・アドレスに関連付けられているその他の名前を表示できます。

分散デプロイメントでは、組織の中の 1 つのノードを対象とする関係を表示することが選択できます。

手順

1. 復元グリッドにある文書のリストから結果を選択し、 「**デジタル・インプレッション (Digital Impression)**」タブをクリックします。
2. 調べたい項目をリストから選択します。

   デフォルトでは、デジタル・インプレッション・レポートは、ID の種類ごとに編成されて表形式でリストされます。中心 ID と対話したすべての ID が表示されます。対話相手の ID は ID の種類ごとに編成され、対話の頻度でソートされます。

3. 目的の ID を見つけたら、それを選択します。

   ID はハイパーリンクになっていて、別のレポートの中心 ID として使用できます。別のタブが作成され、新しい中心 ID が表示されます。選択した疑わしい攻撃者の対話相手を表示し、さらにその対話相手の対話先を表示することができます。さらなる疑わしい攻撃者やエンティティー、およびそれらの対話相手に調査の範囲を広げることができます。

4. 別のホストを調べるには、「**リモート・ホストの選択 (Select Remote Host)**」リストから IP アドレスを選択します。

   分散インストール済み環境では、QRadar Incident Forensics ホストを選択するとデジタル・インプレッションを表示することができます。デフォルトの表示はプライマリー・ホストですが、QRadar Incident Forensics ホストに関連する任意のセカンダリー・ホストを選択することができます。

5. 中心 ID から他の ID への対話の関係を視覚化するには、「**データの視覚化 (Visualize Data)**」タブをクリックします。

視覚化ツール

複数の属性およびデータ・カテゴリーにわたって視覚的に関係を調べることができます。

1 つ、2 つ、または多数選択した文書のメタデータの関係マップを参照するには、「視覚化 (Visualize)」ウィンドウを使用します。多数選択した文書を使用した場合は、メタデータの関係および相対頻度が包括的に表示されます。調査担当者は、これらのパスをたどって、セキュリティー・インシデントの調査を進めることができます。

選択した文書の視覚化は、1 つまたは両方の関係を変更することで、別の関係を使用して容易に再構成することができます。

視覚化では、選択した文書の中に含まれるすべての関係と、関係の頻度が表示されます。各ノードは、選択した文書にあった関連する個々のメタデータを表します。サイズは、他のノードと比較した場合の相対的な頻度を表します。リンクは、個々のメタデータの間で検出されたつながりを示し、サイズでその頻度を表します。調査担当者は、ノードを使用してその後の調査のために可能な手段を特定できます。

関係の視覚化

復元した文書の属性間の関係を参照するには、 「視覚化 (Visualize)」ウィンドウを使用します。例えば、特定の E メール・アドレスと通信した E メール・アドレスを調べることができます。

手順

1. 復元グリッドで、調査する文書のチェック・ボックスをクリックして「**視覚化 (Visualize)**」をクリックします。
2. レイアウト、表示する文書の数、および調べる属性間の関係を選択し、「最新表示」をクリックします。
3. 画像の詳細度を調整するには、ズーム・コントロールを使用します。

4. 新しい検索を実行するかアクティブ・フィルターを変更するには、ノードを右クリックします。

   コンテキスト・メニューから、そのメタデータを元に戻して新しい検索を実行することができます。また、アクティブ・フィルターを変更してそのメタデータを含めるか除外することもできます。

   制約事項: 1 つの「視覚化 (Visualize)」ウィンドウに一度に 9999 件までの文書を表示することができます。

疑わしいコンテンツや悪質なコンテンツについての成果物分析

セキュリティー・アナリストは、ファイルや画像などの再構成された成果物を分析することで、検出を回避した脅威を見つけることができます。また、共謀者と成果物の間のつながりを理解するために、これらのファイルや画像との間のリンクも調査することができます。

例 - 攻撃元を見つけるための成果物分析の使用 (最初に感染したマシン)

John は Replay Industries のセキュリティー・アナリストです。セキュリティー対策を実施しているにも関わらず、いくつかのシステムが感染しています。John はこれらのシステムを識別して検疫した後で、これらのシステムがどのように感染したのか、および他の資産が同様に危殆化しているかどうかを調べる必要があります。

IP アドレスからのパケットの復元

IP アドレスおよび関連するおおよその時間フレームを始めとして、John は QRadar Incident Forensics を使用して関連するパケット・データを復元することができます。

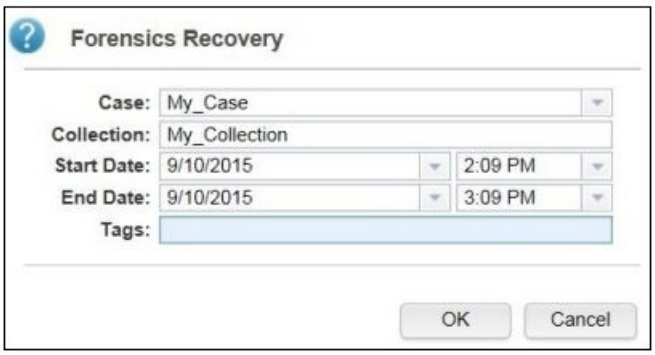


図 1. IP アドレスからの復元

ファイル分析

John は実行可能なコンテンツを探しているので、QRadar Incident Forensics に組み込まれているファイル分析機能を使用することから始めます。これで John は、すべてのファイル、それらが送信された頻度、それらに埋め込みのファイルやスクリプトが含まれているかどうか、およびそれらのエントロピー・スコアのリストを見ることができるようになりました。John は、QRadar Incident Forensics が疑わしいコンテンツとして、および埋め込みスクリプトを持つものとしてフラグを立てた画

像ファイルを素早く確認できます。

Doc #	File Name	Extension	Description	Protocol	Frequency	Suspect Content	Embedded Script	Embedded Files	File Size (Bytes)	File Hash (SHA-256)	Entropy
1	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	1916	70c6e673cd0150b1ffa89e	4.93731
2	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	163060	dbbb35dcf2e494f068b9d1	5.74523
3	index.php	php	JavaScript	http	1	No Suspect Content	No Embedded Script	0	164112	909a0b9fa48182b58dd85	5.38451

図 2. ファイル分析の属性

データのランダム性を測定し、暗号化されたマルウェアを見つけるために使用されるファイル・エントロピー・スコア、およびエントロピー分布にも、ファイルの一部があるべき姿ではないことが明確に示されます。さらなる分析によって、このファイルには、既存のセキュリティー対策の検出から逃れて、システムが感染する原因となった、新しい形式のマルウェアが含まれていることが証明されます。

以下の図では、バイトあたりのビットの変動性の指標としてエントロピーが使用されています。データ・ユニット内の各文字は 1 バイトから成るため、エントロピー値はそのデータ・ユニットの文字の変動および圧縮性を示します。ファイル内のエントロピー値の変動は、ファイル内に疑わしいコンテンツが隠されていることを示す可能性があります。例えば、高いエントロピー値は、データが暗号化および圧縮されて格納されていることを示す可能性があります。低いエントロピー値は、実行時にペイロードが暗号化解除され、別のセクションに格納されていることを示す可能性があります。

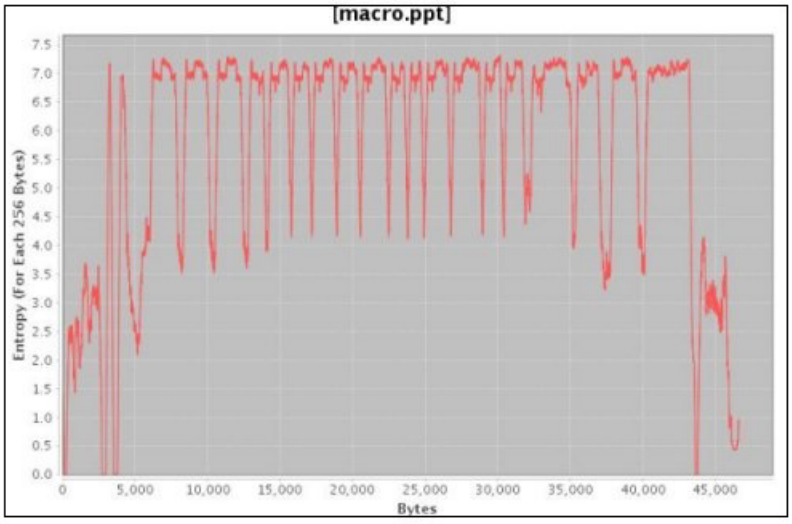


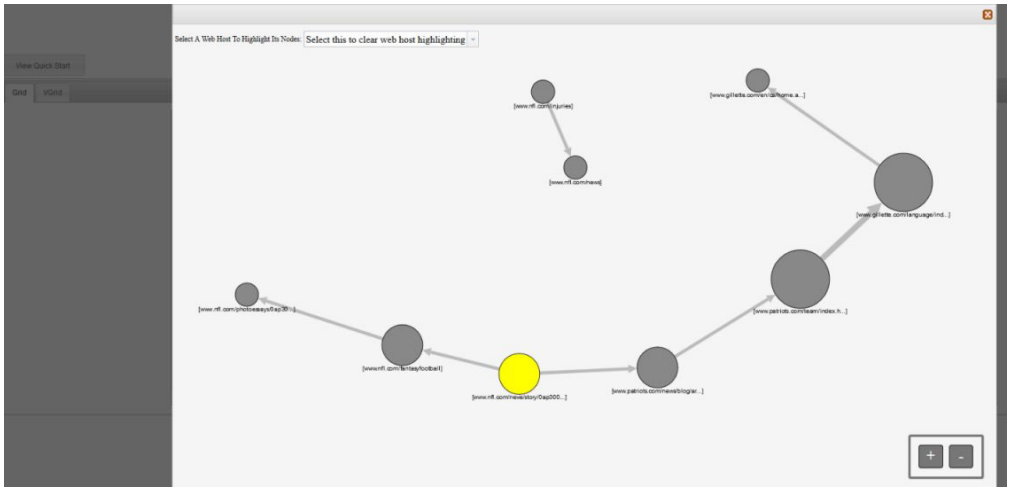
図 3. 埋め込みスクリプトを示すファイル・エントロピー・グラフの例

John は今度は、どこからのこのファイルが現れ、他に誰がこのファイルを持っている可能性があるかを知る必要があります。John は QRadar Incident Forensics を使用して、感染した画像ファイルを提供する Web サーバー素早く見つけます。問題の Web ページは、誰もがお気に入りの NFL チームの最新ニュースをブロードキャストすることで人気があり、危殆化しています。このWeb サイトには多くの画像が含まれていますが、対象は John がファイル分析を使用して先ほど見つけた、埋め込みマルウェアを含んだ画像 1 点だけです。

Web サイトの通信を視覚化するリンク分析

他のどのシステムが影響を受けている可能性があるかを判別するために、John はリンク分析を使用して、閲覧されたすべての Web サイトを素早く可視化します。Replay 社が取引をした企業の Web サイトにわたる大量のトラフィックに関わらず、感染した Web ホストに対するほんの一部のアクセスが、明確に見られる場合があります。John はこれらのリンクを分析して、ネットワーク上の他のどのサーバーがこの Web ホストにアクセスするために使用されたかを確認します。

調査において John は、Web ページを表すノードと、Web ページ間の関係またはトランザクションを表すノード間の矢印をグラフ内で使用して、トラフィック・パターンに素早くアクセスし、どのように文書がトラバースしたかを確認します。ノードが大きいほど、その文書のパスにより多くのリンクがあり、リンク矢印が大きいほど、そのリンクがより多くの回数使用されています。



人気のある NFL ニュース・サイトになると、他の多くのサーバーがその Web ホストに接触しており、潜在的に影響を受けていることを確認するのは、驚くことではありません。

画像分析

どのサーバーが悪意のある画像ファイルをダウンロードしたかを絞り込むために、John は画像分析に切り替えて、送受信されたすべて画像ファイルを素早く確認することができます。

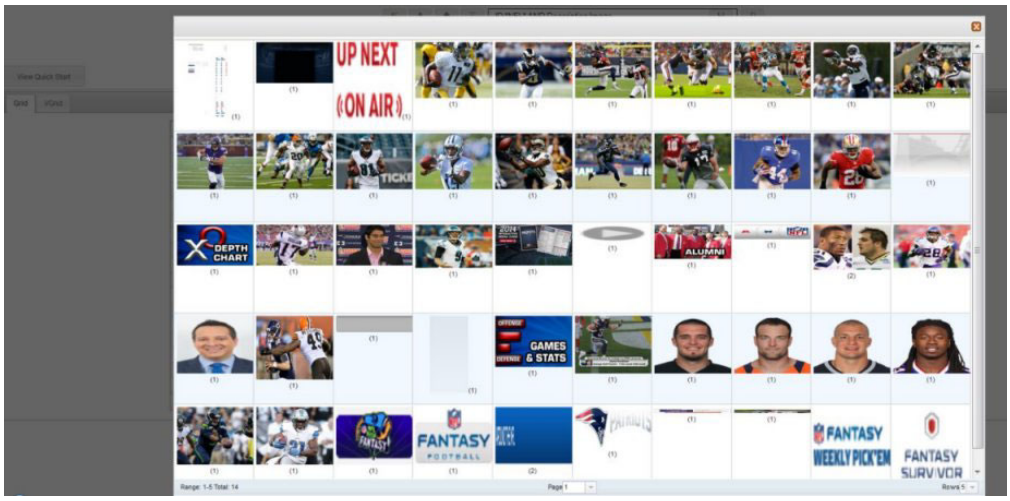


図 4. 画像分析と画像の分布の例

John は、すべての感染したサーバーと、彼が気付いていなかった 2 つのサーバーを素早く確認します。これらのサーバーはすべて危殆化した画像ファイルにアクセスしていました。

John は、同じ Web サイトにアクセスした他のいくつかのサーバーが、感染したファイルをダウンロードしなかったことも判別します。John はこれら 2 つの追加サーバーを検疫し、Replay Industries が IBM X-Force® Exchange にアップロードして他と共有できる、感染したファイルの新しいファイル・ハッシュを作成する必要があるという情報を得ました。

埋め込みコンテンツと悪意を持つアクティビティーについてのファイルの分析

隠れた脅威についてファイルを調査するために、ファイル・エントロピー値を調べて、さらなる分析のために埋め込みのファイルやスクリプトをダウンロードし、文書とその属性を表示することができます。

侵入者はコンテナー・ファイル内のバイナリー・ファイルのコンテンツを難読化できるため、IBM Security QRadar Incident Forensics のファイル分析を使用して、ファイルに埋め込みスクリプトや他のバイナリー・コンテンツが含まれているかどうかを検査できます。

ファイル・エントロピー は、ファイル内のデータのランダム性を測定し、ファイルに隠しデータや疑わしいスクリプトが含まれているかどうかを判別するのに使用されます。ランダム性の尺度は、ランダムでないことを示す 0 から、暗号化されたファイルなど完全にランダムであることを示す 8 までです。ユニットをより圧縮できるほど、エントロピー値は低くなります。ユニットをより圧縮できないほど、エントロピー値は高くなります。

以下の図では、バイトあたりのビットの変動性の指標としてエントロピーが使用されています。データ・ユニット内の各文字は 1 バイトから成るため、エントロピー値はそのデータ・ユニットの文字の変動および圧縮性を示します。ファイル内のエントロピー値の変動は、ファイル内に疑わしいコンテンツが隠されていることを示す可能性があります。例えば、高いエントロピー値は、データが暗号化および圧縮

されて格納されていることを示す可能性があります。低いエントロピー値は、実行時にペイロードが暗号化解除され、別のセクションに格納されていることを示す可能性があります。

手順

1. 「**Forensics**」タブの「**グリッド (Grid)**」ビューから、リカバリーされたファイルを 1 つ以上選択します。
2. グリッドの上部にある調査ツールのメニューで、「**ファイル分析 (File Analysis)**」をクリックします。

   結果では、グリッドの各行には文書の分析データが含まれています。例えば、ファイル名、説明、疑わしいコンテンツが検出されたかどうか、およびエントロピー値などです。
3. エントロピーなどの特定の属性でファイルをソートするには、関連付けられている列見出しをクリックします。
4. ファイルのリストから、さらなる調査のためのファイルを右クリックします
   - 文書とその属性をレビューするには、「**文書の表示 (Display Document)**」をクリックします。
   - エントロピー・グラフをレビューして、埋め込みのファイルやスクリプトにマルウェアが含まれる可能性があるかどうかを確認するには、「**エントロピーの表示 (Display Entropy)**」をクリックします。

     ファイルに悪質なコンテンツが含まれている可能性があるかどうかの指標として、エントロピー値を使用できます。例えば、ASCII テキスト・ファイルは一般的に圧縮性が高く、エントロピー値が低いです。暗号化データは一般的に圧縮性がなく、通常はエントロピー値が高いです。多くの場合、マルウェアはファイルと画像の両方の中に圧縮され隠されています。
   - 埋め込みファイルをダウンロードするには、「**埋め込みファイルの抽出 (Extract Embedded Files)**」をクリックし、ダウンロードするファイルを選択します。

     このオプションは、埋め込みのファイルやスクリプトを持つ文章でのみ有効です。ファイルは、ご使用の Web ブラウザーのダウンロード・ロケーションにダウンロードされます。潜在的に危険なスクリプトを保護されていない環境で開かないように注意してください。

隠れた脅威や疑わしいアクティビティーについての画像の分析

表示された画像は、サイズと、括弧内の頻度の数との関連性でソートされています。この分析は、従業員が会社のリソースを使用して不適切な画像、制限された画像、または禁止された画像を見ている場合に役立つ可能性があります。例えばこれらの画像は、セキュリティー侵害のターゲットである飛行機、特定のビル、または場所に関連している可能性があります。

画像分析を使用して、1 つ以上のパケット・キャプチャー・ファイル内にある 1 つ以上の文書から、最も関連する画像を、各文書を開いて画像を表示する代わりに 1 つのディスプレイで表示することができます。

手順

1. 「**Forensics**」タブの「**グリッド (Grid)**」ビューで、説明内に画像を含む文書を 1 つ以上選択します。
2. グリッドの上部にある調査ツールのメニューで、「**画像分析 (Image Analysis)**」をクリックします。

   結果では、文書内に含まれているすべての画像のサムネール版が関連性の順序で表示されます。画像の隣にある括弧内の数字は、文書内の画像のインスタンス数を示します。サムネール・イメージの上にカーソルを移動すると、画像が大きくなります。
3. さらに調査するには画像を右クリックします
   - 画像とその属性をレビューするには、「**文書の表示 (Display Document)**」をクリックします。
   - エントロピー・グラフをレビューして、画像にマルウェアが含まれている可能性があるかどうかを確認するには、「**エントロピーの表示 (Display Entropy)**」をクリックします。

     ファイルに悪質なコンテンツが含まれている可能性があるかどうかの指標として、エントロピー値を使用できます。例えば、ビットマップ画像ファイルおよび ASCII テキスト・ファイルは一般的に圧縮性が高く、エントロピー値は低いです。暗号化データは一般的に圧縮性がなく、通常はエントロピー値が高いです。多くの場合、マルウェアはファイルと画像の両方の中に圧縮され隠されています。

接続と関係についてのリンクの分析

リンク分析では、リンクは閲覧された Web サイトの間の共通性を示します。セキュリティー・インシデントの調査中に、オーバーラップがある場所と、個人がどのように通信しているかを素早く確認できます。

例えば、加害者のグループが協力していると思うが、その方法が分からない場合、多数のユーザーからの一連の文書を調べて、リンク分析を使用して共通 Web ページを表示します。その後、特定の Web サイトを調査することができます。

手順

1. 「**Forensics**」タブの「**グリッド (Grid)**」ビューから、Web ページを 1 つ以上選択します。
2. グリッドの上部にある調査ツールのメニューで、「**リンク分析 (Link Analysis)**」をクリックします。

   Web サイト間に関係がある場合は、Cytoscape グラフにそれらの Web ページが円 (ノード) として表示され、Web ページの間のリンクが矢印として表示されます。ノードが大きいほど、その文書のパスにより多くのリンクがあり、リンク矢印が大きいほど、そのリンクがより多くの回数使用されています。選択されたノードは黄色で表示されます。
3. 特定の Web ホストからの通信を調査するには、「**Web ホストの選択 (Select Web Host)**」リストでその Web ホストを選択します。

選択した Web ホストの Web ページを表すノードは、濃い灰色の円として強調表示されます。

4. 円 (ノード) や矢印のサイズを拡大したり縮小したりするには、ズームイン (+) コントロールまたはズームアウト (-) コントロールを使用します。

   また、マウス・ホイールをスクロールアップしたりスクロールダウンしたりして、ノードや矢印のサイズを拡大したり縮小したりすることもできます。

5. 1 つ以上のノードを移動させるには、ノードをクリックしてドラッグします。

   背景の任意の場所をクリックしたままドラッグすることで、グラフ全体を移動できます。

文書の 「属性」ページからのリカバリーの実行

ある文書の「**属性**」タブが表示されているときに、1 つの IP アドレスまたは 1 つのポートに対してリカバリーを実行できます。

手順

1. 「**Forensics**」タブの「検索」ページから、検索を行います。
2. 返された文書のリストから 1 つをクリックして、それを開きます。
3. 「**属性**」タブをクリックします。
4. IP アドレスまたはポートをクリックします。
5. メニューから、「**リカバリーの実行 (Run Recovery for)**」をクリックします。

第 5 章 IP アドレスに対するネットワーク・トラフィックの調査

セキュリティー・インシデント中に行われた会話での関連するコンテントを視覚化するために、IP アドレスに関連したネットワーク・トラフィックを復元して再構成することができます。IP アドレスに関連する既存のケースを検索することもできます。

IP アドレスからネットワーク・トラフィックを再構成すると、インシデントが作成されます。調査担当者は、セキュリティー・インシデントに由来する一連のイベントを視覚化したり、インシデントの文書を表示したりすることができます。

IBM Security QRadar Incident Forensics は、使用可能なすべてのネットワーク・データ、ファイル・データ、メタデータ、および復元された各ファイルにあるテキスト文字に索引を付けます。

分散デプロイメントでは、複数のキャプチャー・デバイスおよび QRadar Incident Forensics ホストがデータを収集して処理します。集約されたインシデント復元結果や、ホストおよびキャプチャー・デバイスによる結果を表示することができます。

手順

1. ケースを作成し、パケット・キャプチャー・デバイスからデータを取得するには、QRadar で IP アドレスを右クリックした後に、「**Forensics Recovery の実行**」を選択します。
   a. データ復元パラメーターについて以下の表で説明します。

表 5. データ復元のパラメーター

パラメーター	説明
ケース	調査に使用するケース。 **制約事項:** ケース名は固有でなければなりません。
コレクション	復元したデータをコレクションにグループ化し、ケースに関連付けます。 **制約事項:** コレクションの名前は固有でなければなりません。そのコレクション名がケースに存在する場合は、元のコレクションが削除されます。
開始日	データ・パケット収集の開始日時。
終了日	データ・パケット収集の終了日時。
タグ	関連した文書から正確な結果セットを迅速に得るために使用するメタデータ・タグ。 **制約事項:** # 記号は許可されていません。$、%、* などの他の特殊文字は使用できます。

   b. 「**OK**」をクリックしてから「**Forensics**」タブをクリックします。

トラブルシューティング: 「データをリカバリーする許可がありません」という内容のメッセージが表示された場合は、ご使用のセキュリティー・プロファイルにその IP アドレスへのアクセス権限があることを確認してくださ

い。場合によっては、「**タグ**」フィールドに # 文字を使用したときに、このメッセージが表示されることがあります。

c. 三角形のアイコンをクリックするとインシデントが表示されます。

d. インシデントの一連のイベントを視覚化するには、「**Surveyor ページ結果に移動 (Jump to surveyor page results)**」をクリックします。

e. インシデントの文書を表示するには、「**検索ページ結果に移動 (Jump to search page results)**」をクリックします。

2. IP アドレスの既存のケースを検索するには、QRadar で IP アドレスを右クリックし、「**Forensics Search の実行**」をクリックします。

a. 「**Forensics**」タブでインシデント (三角形) のアイコンをクリックします。

b. インシデントに関連したアクティビティーを集約したものを調査するには、ケースの上にマウス・ポインターを移動して強調表示した後、検索アイコンをクリックします。

c. 分散デプロイメントの QRadar Incident Forensics ホストおよびキャプチャー・デバイスによるアクティビティーを調査するには、「**ケース**」エントリーを展開して「**集合 (Collection)**」エントリーを展開します。

d. インシデントでの対話を日時順のリストとして表示するには、コレクションの上にマウス・ポインターを移動して強調表示した後、Surveyor のアイコンをクリックします。

関連概念:

27 ページの『再構成された文書の表示』

「**表示 (View)**」タブには、「リスト」ビューの画面の左側で選択した文書の再構成されたものが表示されます。

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。

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。

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

この用語集には、IBM Security QRadar Incident Forensics 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、以下の相互参照を使用します。

- *「を参照」*は、非優先用語の場合は優先用語を、省略語の場合は省略していない形式を読者に示すものです。
- 「～も*参照*」という表記は、関連する用語や対照的な用語を参照するように促すための表記です。

その他の用語および定義については、IBM Terminology Web サイトを参照してください (新規にウィンドウが開きます)。

『A』 『B』 『C』 46 ページの『D』 46 ページの『E』 46 ページの『F』 46 ページの『H』 46 ページの『I』 46 ページの『M』 46 ページの『O』 47 ページの『P』 47 ページの『R』 47 ページの『S』 47 ページの『T』 47 ページの『V』

A

異常 (anomaly)
正常なネットワーク動作から逸脱した動作。

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。攻撃者 (attacker) も参照。

攻撃者 (attacker)
情報システムに害を及ぼそうとしたり、一般アクセス向けではない情報にアクセスしようとしたりするユーザー (人間またはコンピューター・プログラム)。攻撃 (attack) も参照。

B

ブール演算子 (Boolean operator)
一連の演算を評価するときに AND、OR、または NOT という論理演算を指定する組み込み関数。ブール演算子には &&、||、および ! がある。

階層リンク (breadcrumb)
サイト内でのユーザーの位置を表示する Web インターフェース・エレメント。通常、ページの上部または下部に表示される一連のハイパーリンク。これらのリンクは、ユーザーが開始位置に戻れるように、表示したページを示す。

C

キャプチャー・デバイス (capture device)
パケット・キャプチャー・アプライアンス (packet capture appliance) を参照。

ケース (case)
特定の調査に関連するデータベース内に含まれている情報。

カテゴリー (category)
特定の説明または分類に従ってグループ化されている項目の集合。カテゴリーは、ディメンション内のさまざまなレベルの情報である場合もある。

中心 ID (centering identifier)
その他すべての ID が対話するカテゴリー項目。中心 ID は、調査の中心的な項目である。

コレクション (collection)
ケースに関連付けられている、データの固有の名前付きセット。例えば、キャプチャーしたネットワーク・パケットの順序セット。

継続的に収集された電子的存在 (continuously collected electronic presence)
リンクされているデジタル・インプレッションのコレクションとしての攻撃者のオンライン ID。

会話 (conversation)
フォレンジックに再構成した、2 つ以上のネットワーク・エンドポイント間のデータのフロー。例えば、ソーシャル・ネットワークの会話。

D

デキャップ (decapping)
取り込まれたすべてのデータが結果レポートに反映されるように、パケット・キャプチャー・データを逆コンパイルするプロセス。

デジタル・インプレッション (digital impression)
個々のケース内で相互に関連するタグ付き ID から成るレポート。

ディジタル・インプレッション関係 (digital impression relationship)
1 つのケースに関連するタグ付き ID 間の関係。

Domain Inspector
特定のドメイン Web サイト (Facebook、Gmail など) からフォレンジック・データを逆構造解釈して抽出するために設計された特殊なインスペクター。

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。

F

フロー・レコード (flow record)
2 つのホスト間の会話のレコード。

フォレンジック調査担当者 (forensic investigator)
ネットワーク・トラフィックおよびフォレンジック・リポジトリー内の文書から関連するデータを抽出するユーザー。

H

仮説 (hypothesis)
ケースで収集された使用可能な証拠に基づいて、インシデントに対して提起された説明。仮説は検証可能かつ反証可能である必要がある。

I

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。

インシデント (incident)
セキュリティー・インシデント (security incident) を参照。

取り込まれたネットワーク・トラフィック (ingested network traffic)
Forensics のデキャップ・プロセスによって処理されたキャプチャー済みネットワーク・トラフィック。

M

メタデータ (metadata)
データの特性を説明するデータ。説明的データ。

メタデータ関係マップ (metadata relational map)
ケース文書の関連するメタデータを表示するマップ。

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。

P

パケット・キャプチャー・アプライアンス (packet capture appliance)
トラフィック・データをインターセプトしてログに記録するスタンドアロン・アプライアンス。

パケット・キャプチャー情報 (packet capture information)
キャプチャー・デバイスによって収集されたトラフィック・データ情報。

Protocol Inspector
ネットワーク・プロトコル (HTTP、FTP など) からフォレンジック・データを抽出するために設計された特殊なインスペクター。

R

リカバリー・ジョブ (recovery job)
照会されたキャプチャー・データをリカバリーして、取り込みのためにデキャッパー・デバイスに転送するプロセス。

S

セキュリティー・インシデント (security incident)
正常なネットワーク運用が侵害されたり、危険にさらされたり、攻撃されたりするイベント。

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。

Surveyor ツール (surveyor tool)
1 つのセキュリティー・インシデント内のアクティビティーを日時順にビジュアライザーに表示するツール。

T

トラフィック (traffic)
データ通信で、パス内の特定のポイントを通過して伝送されたデータ量。

証跡 (trail)
ケースに関与した個人をケース外部の個人につなげるデジタル・インプレッション。

V

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。

[カ行]

[サ行]

[タ行]

[ハ行]

[マ行]

[ヤ行]

I