IBM Security QRadar Incident Forensics

ネットワークの可視化により、悪意のあるアクティビティーを素早く徹底的に調査

ハイライト

- 企業ネットワーク全体のパケットをキャプチャーして、セキュリティー・インシデントを調査
- インターネット検索エンジンに類似したインターフェースでクエリー・プロセスを簡素化
- IBM® Security QRadar ソリューションと既存のパケット・キャプチャー (PCAP) 形式を統合して、データのデコードやインデックス作成、再構築、分析を実行
- 関連性、タイムライン、ソース、脅威カテゴリーなど、データに関するさまざまなビューを生成
- 疑わしいコンテンツへのラベル付け、URL 分類の追加、ユーザーやアプリケーションに関するデジタル・インプレッションの表示により、新しいインテリジェンスを構築
- 特定したインシデントの解決 (数日、数週間ではなく、多くの場合、数分から数時間で対応) を支援

IBM Security QRadar Incident Forensics は、セキュリティー・インシデントに関連するネットワーク・アクティビティーをより明確に可視化し、企業の IT セキュリティー・チームに提供するよう設計されたソリューションで、ソフトウェアとアプライアンスをベースに構成されています。この洞察は、広範なネットワーク・セキュリティー・インシデントの発見、損害の修復、データ漏えいや過去に起こったセキュリティー侵害の再発可能性の低減に役立てることができます。

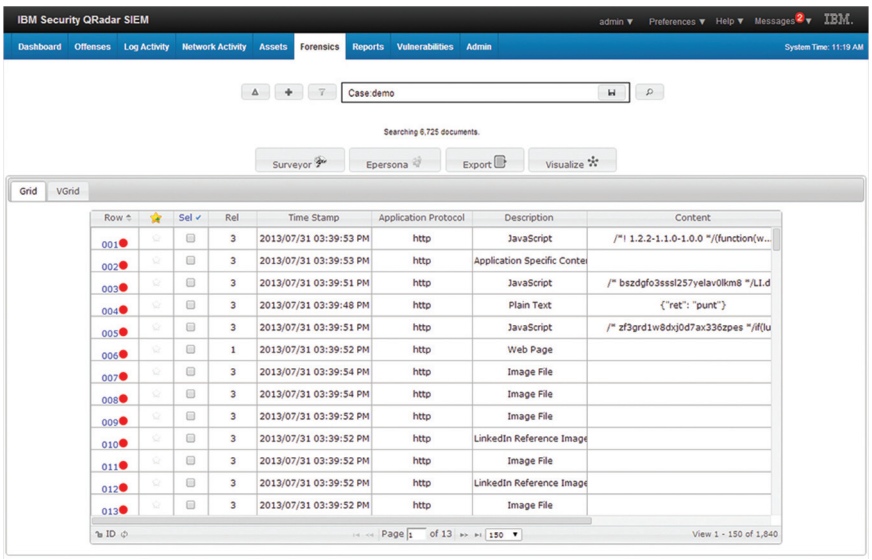
脆弱 (ぜいじゃく) 性があまりに多く存在し、手作業でセキュリティー侵害の調査や修復をするには人手が足りない今日の企業環境で、QRadar Incident Forensics は、ソース・イベントとネットワーク・フロー詳細のログ記録を使用しただけでは得ることのできない洞察と分析を提供します。ソリューションには、IT セキュリティー・チームの素早くスマートな意思決定を支援する、強力なインデックス作成、検索、データ・ピボッティング、レポート作成といった機能があります。

シンプルな検索エンジンに類似したインターフェースにより、セキュリティー・インシデントに関連するデータを直感的に検索できます。データには、保管データ (文書)、移動中のデータ (パケット・キャプチャー)、構造化データや非構造化データが含まれ、文書やファイルには、電子メール・メッセージ、voice-over-IP (VoIP) 通話、閲覧した Web サイト、ブログ記事のほか、メッセージに添付されたファイルや画像なども含まれます。QRadar Incident Forensics は、これらのデータのすべてにインデックスを作成して相関を取り、検索結果に優先順位を付けることで、既存の SIEM 相関規則により生成された誤検出の中から真の脅威を素早く区別できるようにします。生のネットワーク・データを再構成して元の形式に戻し、セキュリティー・インシデントを追跡することで、QRadar Incident Forensics は価値ある情報を提供して、ネットワーク・セキュリティーの保護、外部からの攻撃やインサイダーの脅威の分析と防止、インシデントに関連する証拠の文書化を支援します。

単なるパケット・キャプチャーを超える調査

QRadar Incident Forensics は、IBM QRadar Security Intelligence Platform に、単一コンソールの管理インターフェースでシームレスに統合されます。標準の PCAP 形式と互換性のあるこのソリューションにより、IBM X-Force など外部の脅威情報源の特定した QRadar 攻撃または予想される攻撃状況について、指示的分析調査を行えます。ネットワーク・インフラストラクチャー全体にわたってセキュリティー・インシデントを調査し、可視化します。

QRadar Incident Forensics は、ほかのソリューションと異なり、PCAP からより有益なデータを抽出するだけでなく、関連する文書やファイルをインポートしてこれらのデータもすべて、検索によるデータ探索に包括的に使用できるようにします。メタデータと PCAP の実際のペイロードやファイル文書に



IBM Security QRadar Incident Forensics の検索結果は、ブール値の自由文クエリーとの関連に基づいて優先順位を付けたリストとして表示されます。

インデックスを付ける強力なインデックス作成機能で、検索のパフォーマンスを強化しています。これにより、分析担当者が数字や日付、キーワードを含むテキスト・ベースの検索を実行できるようになります。ソリューションは、疑わしいアクティビティーに関するリアルタイムの調査と、過去の操作の再構築の両方をサポートし、ほとんどの場合、数秒で検索結果を返します。

インシデントに関連するデータの特定と分析の包括的なプロセス

セキュリティー・インシデント調査に使用される QRadar Incident Forensics は、以下の手順や機能を通じてデータとネットワークの関係、イベントのタイムライン、イベントの発行元、脅威カテゴリーといった情報を返します。

- **インデックス付け** - 利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、復元された各ファイルのテキストの文字にまでインデックスを付け、その後、拡張性の高い検索エンジンのインデックス作成システムを使用してすべてを保存します。
- **再構築** - PCAP データに埋め込まれた IP セッションを認識することで、関連する PCAP の生データのすべてを収集し、コンテンツを元の形式に再度組み立て、各セッション、各ファイルのすべてのコンテンツを保持、再構築します。その後、情報を適切なフォーマット (DOC、PDF、PPT、HTML、MPEG3 など) で保存します。
- **検索エンジン** - 検索インターフェースを通じてクエリーを受信すると、アクティビティーや資産のリストをクエリーの結果により優先順位を付けて返します。これらには、チャットの会話、ファイル転送、閲覧した Web ページ、スプレッドシートなども含まれます。
- **検査モード** - クエリー応答時、QRadar Incident Forensics は、やりとりを時系列に表示します。
- **表示** - 検索エンジンの返した結果を開くと、結果に含まれた資産は、ネイティブ・フォーマットで表示されます。ソーシャル・ネットワークや、写真やファイルの交換サイトなどの Web サイトは、再構成された要素がオンラインで表示されているかのように表示されます。
- **データ・ストレージ** - ユーザーの定義した期限を過ぎた膨大な PCAP の生データではなく、調査中に作成された情報のみが保持されるので、ストレージ容量の増加を抑え、セキュリティー・インシデントをより長期的に分析できます。
- **視覚的探査** - セキュリティー分析の際は、複数の属性にまたがる関連性や関係性が視覚的に表示され、調査のニーズに応じて、あるデータ・カテゴリーから別のカテゴリーへ効率的に移動できます。

ビッグデータ分析で得られる重要な洞察と情報

IT セキュリティー・チームが、疑わしいコンテンツを特定し、新しい相関規則を定義し、URL の評価に基づいてコンテンツを分類し、ネットワークの関係を示すデジタル・インプレッションを構築する上で QRadar Incident Forensics は役立ちます。強力なデータ・ピボッティング機能により、IP アドレスや MAC アドレス、電子メール・アドレス、アプリケーション・プロトコル、ユーザー・クエリー、SSL 認証といった検索可能な変数の幅広い関係、時には見つけにくい関係を明らかにできます。

ソリューションは、ビッグデータ分析機能により、3 つの主要領域について重要な洞察や情報を返します。

- **デジタル・インプレッション** - QRadar Incident Forensics は、ネットワークにおける関係を視覚的に再構築して、攻撃元の主体やユーザー、通信方法、通信内容を明らかにします。
- **疑わしいコンテンツ** - あらかじめ構築された規則は、データ・パターンや既知の振る舞いを利用して、再構築されたコンテンツが疑わしいかどうかを識別します。
- **コンテンツの分類** - メタデータに基づいて PCAP コンテンツを動的に分類し、組織が提供する X-Force などの情報フィードを使用して自動的にフィルタリングできるようにします。カテゴリー別にフィルタリングすることで、生産性とパフォーマンスも向上します。

IBM をお勧めする理由

QRadar Incident Forensics の素早い応答と情報提供により、IT セキュリティー・チームは、多くの場合数日かかっていた QRadar SIEM の攻撃記録の調査時間を数時間または数分にまで短縮できます。インシデントが法的な脅威として特定されたら、セキュリティー・チームは、侵入者の操作を 1 つずつ追跡し、セキュリティー侵害に関連するアクティビティーを修復し、操作を無効にして再発を防止できます。

絶えることのない高度な脅威、またはインサイダーの脅威や不正行為に対応する中で、QRadar Incident Forensics は、規制対応の文書化についても IT チームを支援します。セキュリティー・チームでは、誤検出と真の脅威や攻撃を素早く区別する能力が劇的に向上します。また、ネットワーク・セキュリティー・インシデントをより深く理解し、ベスト・プラクティスのセキュリティー・アプローチをプロアクティブに策定できるようになります。

詳細情報

IBM Security QRadar Incident Forensics の詳細については、日本 IBM の営業担当員またはビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。
ibm.com/software/products/ja/qradar-incident-forensics/

日本アイ・ビー・エム株式会社
〒103-8510東京都中央区日本橋箱崎町 19-21

Produced in Japan
April 2014

Please Recycle

WGD03033-JPJA-00