IBM X-Force Exchange

セキュリティー・アナリストが脅威情報を調査し、共有する方法が変わります

特長

- インタラクティブなプラットフォームを通じた最新の脅威の調査
- コレクションの作成によるインシデント調査
- 他の担当者とのコラボレーションによる優先すべき脅威情報の特定
- インテリジェンスの施行を推進

IBM® X-Force® Exchange はクラウド・ベースの脅威情報共有プラットフォームです。これによりユーザーは最新のグローバルなセキュリティー脅威を素早く調査し、実行可能なインテリジェンスを集約し、専門家と相談して、他の担当者とコラボレーションすることができます。IBM X-Force Exchange は人間とマシンのそれぞれが生成したインテリジェンスによってサポートされており、世界的な民間セキュリティー研究機関である IBM X-Force を利用して、ユーザーが新たな脅威に対して事前対応できるように支援します。

多くの企業が外部の脅威情報を使用してセキュリティーに関する意思決定を強化していますが、これには外部の脅威情報を最大限に活用するために必要である重要なサポートが欠けています。セキュリティー・チームは脅威を特定するために複数の情報源を使用していますが、こうした情報源の使用には時間がかかる可能性があり、それらが必ずしも信頼できるとは限りません。重大な影響を与えられるほど素早く情報を処理することができないため、十分にセキュリティー保護を行えないということもしばしばあります。

IBM X-Force Exchange は以下を提供します。

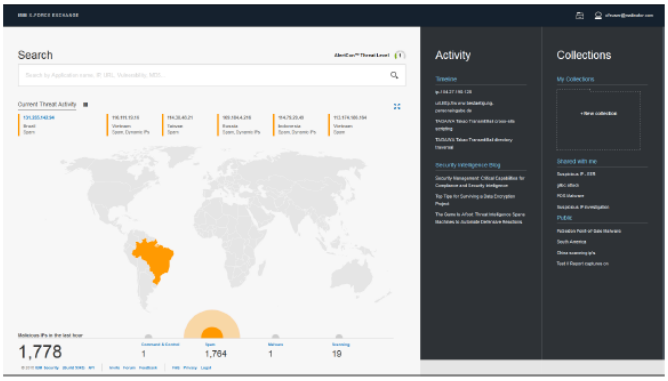
- 大量の脅威情報データにアクセスできる堅固なプラットフォーム
- 人間とマシンのそれぞれが生成した洞察を組み合わせて生み出される脅威インディケーターのコンテキスト
- 脅威の迅速な検出とその対応を支援する統合されたソリューション
- 脅威情報を共有するためのコラボレーション型プラットフォーム
- 検出項目を整理し、注釈付けするための使いやすいインターフェース

さまざまな情報源から収集、整理、要約、公開（共有）された脅威情報

IBM X-Force Exchange は、クローラー・ロボット、ハニーポット、ダークネット、スパムトラップからのデータによって裏打ちされタイムリーに収集・公開された脅威情報とマシンが生成した他の脅威情報を提供します。悪意の可能性のある数千のインディケーターが 1 時間ごとに分類され、プラットフォーム内の脅威情報は継続的に更新されます。次のようなデータ・ソースが X-Force Exchange を支えています。

- セキュリティーの既知の脆弱性に関する世界でもっとも包括的なデータベースの 1 つ
- 数十億のセキュリティー・イベントを対象とした毎日のモニタリングから得られる匿名化された脅威情報
- 数百万のエンドポイントから得られるリアルタイムのグローバルな脅威情報
- 数十億の Web ページおよび画像を対象とした脅威のモニタリングに基づくデータ
- 数百万のスパムおよびフィッシング攻撃に関する詳細なインテリジェンス
- 数千の悪意のある IP アドレスに関するレピュテーション・データ

人間のインテリジェンス、つまり業界のセキュリティー担当者、IBM X-Force の調査担当者、および IBM Security の専門家といったセキュリティー専門家が提供する洞察によって、マシンが生成するデータにコンテキストが加わります。



IBM X-Force Exchange のホーム・ページには、最新のクローラー・データ、ならびに検索用語の傾向、最新の脆弱性、プラットフォームにおける最新のユーザー・アクティビティー、SecurityIntelligence.com が提供する現在のセキュリティーのソート・リーダーシップ・ブログが表示されます。

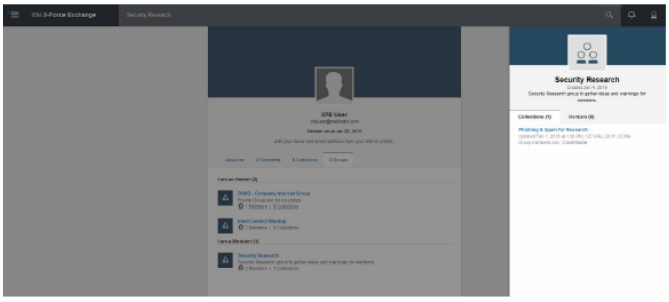
迅速な調査および情報の共有

X-Force Exchange に保管されているデータについてはフリー・テキスト検索が可能であるため、IP アドレス、URL、CVE 脆弱性の数、Web アプリケーション、マルウェア、および IBM ネットワーク保護情報といった、多くのさまざまな脅威の観測対象について、結果を迅速に得ることができます。

また、ユーザーはリスク・レベル (数値と色分けされたもの両方)、不審なアクティビティーのカテゴリー、関連アプリケーション、パッシブ DNS の情報、サブネット、およびマルウェア情報 (使用可能な場合) について、レポートを容易に参照することができます。レポートには、評価の経時的変化といった脅威インディケーターの履歴が表示されます。マルウェア・レポートには、マルウェア・ファミリー、ハッシュ・タイプ、ダウンロード元、およびその他の要素が含まれています。

レポートが作成されたら、ユーザーはコメントを追加して他のユーザー向けにさらに洞察やコンテキストを提供したり、レポートをコレクションに追加したりすることができます。さらに、ユーザーは X-Force チームにフィードバックを提供して特定のレポートの分析をトリガーすることができます。その結果、必要に応じてコンテンツが更新される場合があるのです。

脅威情報に関する他の担当者とのコラボレーションおよび共有



グループとコレクションは、IBM X-Force Exchange 内の重要なコラボレーション・エリアです。

X-Force Exchange プラットフォームによって、業界内の他の担当者と連携して、検出項目の検証および脅威インディケーターの調査を実施できます。IBM X-Force Exchange 内では、ユーザーはコレクションを共有したりレポートにコメントしたりすることによって、他の担当者、IBM Security の専門家、および IBM X-Force の調査担当者などの全員と連携することができます。こうして他の担当者たちとのコラボレーションを通じて脅威にコンテキストを追加することで、有益な情報と無益な情報の切り分けを助け、フォレンジック調査を支援し、グループ間でののインテリジェンスを実現することができます。
ユーザーはグループ機能を使用してプライベート・ワークグループを作成し、コラボレーションと情報の共有を希望する X-Force Exchange ユーザーを選択することができます。グループの所有者はユーザーの追加/除去、グループ・コラボレーションのコレクションの選択、グループ・メンバーへの許可の割り当てを実行できます。

実行可能なインテリジェンスの施行を推進

IBM X-Force Exchange は、IBM Threat Protection System の基礎を形成している脅威情報の上に築かれています。これらの統合により、X-Force Exchange をベースとした実行可能なインテリジェンスが IBM Security 製品に提供されます。また、このプラットフォームはサード・パーティーとの統合に対応するようにも設計されており、脅威情報を自動的に共有するための確立された標準である STIX および TAXII をサポートしています。企業は、基本の鍵認証またはパスワード認証を使用することで、IBM X-Force の脅威情報を自社のセキュリティー製品に関連付けるために、API を活用できます。

ワークフロー合理化のためのケース・ファイル管理の採用

ユーザーはコレクションによって、調査中に収集された脅威情報を集約し、情報を整理し、他のユーザーと共有することができます。コレクションを作成する際、ユーザーは以下のことを実行できます。

- テキスト編集機能による調査の詳細な説明
- 調査に関連する構造化脅威情報レポートの追加。状況を適切に説明するため、レポートを追加する時点での情報のスナップショットを付加できます
- 他の関連コンテンツ (スクリーン・ショット、動画または他のファイルなど) のコンパイル
- コレクションのリンク。関係のある調査間に関連を作成します
- 情報の迅速なアップロードに対応したファイル、コピー・アンド・ペースト、または STIX 形式での脅威情報のインポート

詳細情報

プラットフォームのご使用については、xforce.ibmcloud.com をご覧ください。このオファリングの詳細については、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、www.ibm.com/security/jp/ja/xforce/をご覧ください。

IBM Corporation
Software Group Route 100
Somers, NY 10589

Produced in the United States of America
April 2016