Next Security Inc.

最新のマルウエアや悪意のあるサイト情報をリアルタイムで提供

ThreatIQ

スレットアイキュー

日々巧妙さを増すマルウエアやサイバー攻撃に対し徹底した防御を実現するにはまず「敵」を知ることが重要となります。ThreatIQは、最新のサイバー脅威情報並びにマルウエア検体を毎日お客様に提供する脅威情報サービスです。今世界中にある危険なマルウエアや有害サイトリスト、マルウエアを解析して得られたふるまいや通信ログの詳細レポートを貴社のサイバーセキュリティソリューションに活用すれば、最新の脅威にもリアルタイムで保護できます。また、自社製品に利用して検知性能の評価や強化も行えます。

プロセスと利用構図

① 収集～解析

危険なマルウエアや
有害サイトリストなど

ThreatTrack Security 社

ThreatAnalyzer
クラスタ

マルウエア解析チーム

データはVirusTotalや
Phishtank等のプログラム
パートナーからも提供

② サービス

ThreatIQ

最低でも一日一回新しいフィードが提供されます。

③データ

ThreatIQのフィード(ダウンロードできるデータ)

① マルウェア

② HTTPアラート

③ HTTPブロック

④ フィッシング

⑤ XML

⑥ ボーダーパトロール

⑦ ネットワーク

フィード名	内　訳
① マルウェアフィード	ThreatTrack Security社のレポジトリに集約されたマルウェア検体です。
② HTTPアラートフィード	マルウェアのネットワーク通信ログから得られる通信先URLやIPの一覧です。
③ HTTPブロックフィード	危険と考えられるオンライン上にあるマルウエアへのURLの一覧です。
④ フィッシングフィード	フィッシングサイトの一覧です。
⑤ XMLフィード	ThreatTrack Security社のサンドボックスクラスターで解析されたマルウェア検体のふるまいレポートです。
⑥ ボーダーパトロールフィード	アドウェア、スパイウェア、広告(例: バナー広告、ポップアップ広告等)を配信するドメインの一覧です。
⑦ ネットワークフィード	マルウエアを解析した結果得られたマルウエアが生成するネットワークトラフィックと通信パケットファイルです。

④ダウンロード

～オンプレミスで最新の脅威をリアルタイムで提供～

お客様はThreatIQの7種類のデータを専用FTPサイトからダウンロードし、FTPクライアントはお好きなものをご使用頂けます。ローカルにダウンロードしたデータはお客様のニーズに合わせて自由に加工できます。

お客様の活用事例

各種データをダウンロードすることにより、お客様はサイトでデータベース化してオンプレミスで様々な用途に利用されています。

さらに下記のような応用も ...

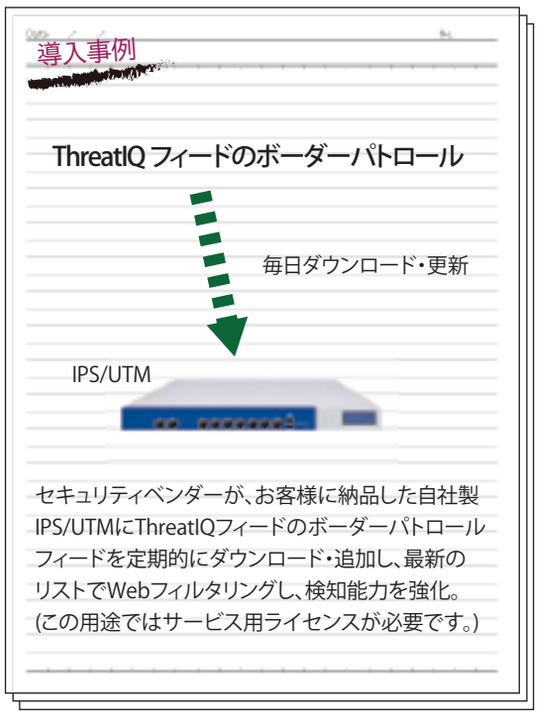
- A社では... 既存のセキュリティゲートウェイの脅威検知能力の強化に。
- B社では... SEIMシステムによるサイバー攻撃分析の補完情報として。
- C社では... 最新のマルウエア研究やサイバー攻撃の分析に。
- D社では... 自社で開発したIPS等のセキュリティソリューションの評価・強化に。
- E社では.. IPSやセキュリティアプライアンスにOEMとして組み込み、最新の脅威に対応した防御能力の強化に。

主な特徴と提供データの詳細

ThreatIQ

特徴

- 今まさに企業を脅かしている世界中の脅威にリアルタイムに対応。
- データは毎日更新され、常に最新の情報を提供。
- 豊富な脅威情報と実際のマルウエア検体。
- 質の高いマルウエアふるまいレポートとネットワークキャプチャレポート。
- データはお使いのFTPクライアントでダウンロードするだけ。
- データは加工しやすい形式となっているため、お客様で自由にデータの加工やカスタマイズが可能。
- 他に類を見ない20TB超の大規模マルウエアレポジトリ。



ライセンス(年間サブスクリプション制です)

■ 企業用ライセンス

ThreatIQフィードを企業内(グループ会社含む)で利用するためのライセンスです。

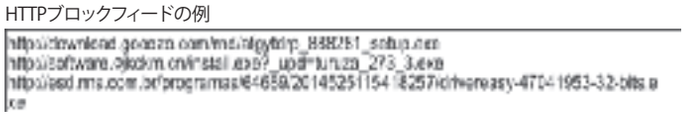
■ サービス用ライセンス

ThreatIQフィードを社内のみならず、社外にあるアプライアンスや社外向けのサービスとして利用するためのライセンスです。

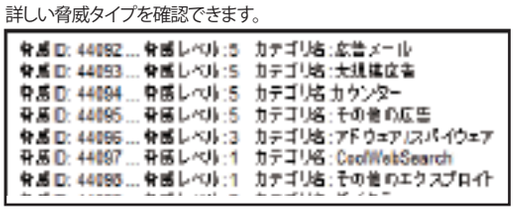
提供されるデータ形式

悪意のあるサイトのURLやドメインの一覧はテキストファイルで提供されます。また、ネットワークトラフィック情報が格納されたネットワークフィードはpcapファイルとしてWireshark等のツールで閲覧できる形でダウンロードできます。マルウエア検体は拡張子を除いた実行可能ファイルの形でありファイル名はハッシュ値となっています。ハッシュ値とマルウエア名の対応表も別途提供されます。

HTTPブロックフィードの例



ボーダーパトロールフィードではさらに細分化され、詳しい脅威タイプを確認できます。



ThreatIQのフィードにはマルウェアの実行ファイルも含まれます。

データ規模

日によって提供されるデータ数が異なります。例えば、マルウェア検体の数は、20,100個、16,000個、20,300個などばらつきがあります。20TB超のデータを保有するThreatIQのデータベースには日々新しいデータが蓄積されています。

一日あたりのデータ数の例

フィード	データ数
HTTPブロックフィード	9,000
HTTPアラートフィード	60,000
フィッシングフィード	18,000
XMLフィード	15,000
ボーダーパトロールフィード	1,150,000
ネットワークフィード	6,000
マルウェア検体	20,000

※提供されるデータには変動があります。

サポート体制

この製品には不明点及び障害と思われる内容についてのお問い合せヘルプデスクが標準価格にバンドルされています。尚本サービスは標準で24時間365日弊社に登録されたグループリーダの方からのお問い合わせを弊社RiMIC(Risk Management Infomation Center)が電話、MAIL, FAX等で対応をさせて頂きます。

ヘルプデスク　IT監視・管理業務
スマートアウトソーシングサービス
RiMIC
RISK Management Information Center

当製品に関する詳細はこちらから ▶ www.next-security.jp/threatiq

販売元：Next Security Inc.
ネクスト・セキュリティ株式会社
〒140-0004　東京都品川区南品川2-4-7アサミビル5階
[東京本社] TEL：03-5783-0702　FAX：03-5783-0734
[大阪事業所] TEL：06-6362-2007　FAX：06-6362-2008
[E-mail]　info@next-security.jp
[Facebook] www.facebook.com/NextSec.inc
[Twitter]　@Next_Security