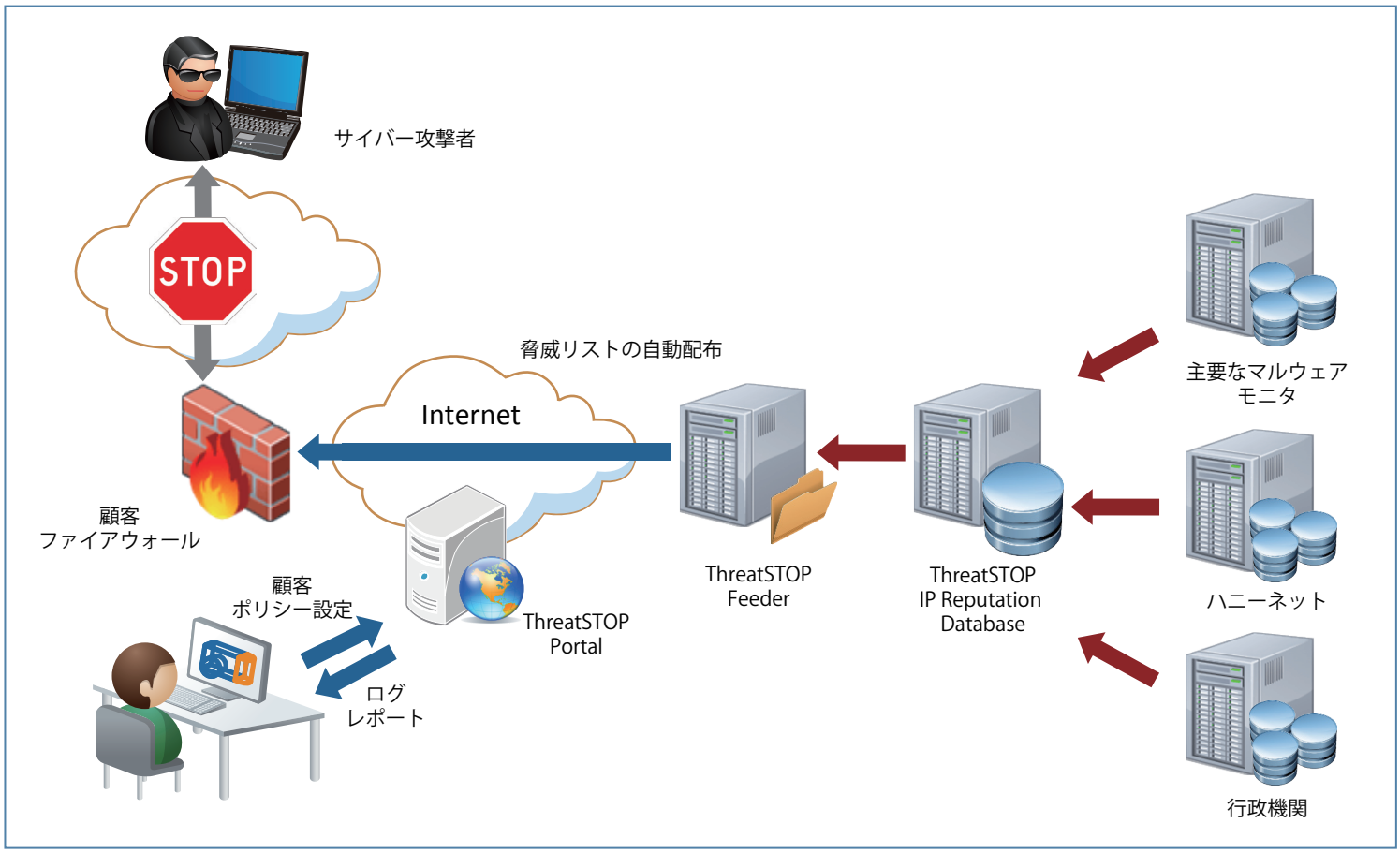
ThreatSTOP

サイバー攻撃に対する多重防御をクラウドで提供する リアルタイムのIPおよびドメインレピュテーションサービス ThreatSTOP

現在、ネットワークの大半がマルウェアに冒されているという調査結果が報告されています。その上、マルウェアはますます高度化し、また増殖しています。また、DDoS攻撃などでサイトを閉鎖せざるをえない事例も多く見かけます。
日々脅威を増すサイバー攻撃に対して様々なツールが提供されていますが、新たな投資や管理を担当する人材を簡単に確保できる企業は多くないのではないでしょうか。
こうした状況に対し、脅威となる攻撃者からの通信や不正なサーバへのアクセスをブロックするサービスをThreatSTOP社は開発および提供します。
ThreatSTOPのリアルタイムのIPおよびドメインレピュテーションサービスは、35を超す主要なマルウェア・モニタおよびハニーネット、行政機関やその他の独自のソースから脅威フィードを集約し、不正なIPアドレスのリストを作成し、DNS（Domain Name System）プロトコルを使用した、パテントを持つ独自の配信メカニズムを用いて既存のファイアウォール等に配布し、マルウェアの侵入および不正な外部サーバへの通信をブロックします。



ThreatSTOPは、脅威となるIPアドレスのリストを様々なソースから収集、データベース化、目的に応じて脅威リストを作成し、DNSの仕組みを利用して顧客機器に配布することにより、マルウェアの侵入や不正な外部との通信をブロックします

◆IPアドレスリスト
Email DNS ブラックリスト、アンチウイルスベンダーなど35以上のソース（Dshield, Spamhaus, 等）から脅威となるIPアドレスを収集し、IPアドレスをスコアリングし、データベース化します。

◆脅威リストの配布
脅威リストの配布にはDNSを利用、ユーザ毎にFQDNドメイン名を割り当て、割り当てられたFQDN名の名前解決をすると脅威リストが顧客機器に配布されます。既存のファイアウォール上でスクリプトを動作させ、当該機器のブロックリストへの反映を行います。

◆レポートの作成
ブロック結果は、ThreatSTOPクラウドへ送信され、そのログからレポートが作成されます。また、ボットネットC&Cサーバへ通信をしようとしたPCの発見も可能です。

ThreatSTOPの特長

●導入方法がシンプルで、総所有コストを低減可能
ThreatSTOPは、ファイアウォールでネイティブに実行されるか、1時間以内に設定できるような簡単なスクリプトで実行されるため、新しい機器を購入したり、既存の、ファイアウォールを置き換える必要がありません。
ネットワーク再設定、テスト、認証、従業員のトレーニング等に係る人手も時間も不要です。

●ゼロディ攻撃を防御
ThreatSTOPは、攻撃シグネチャに依存せず、脅威となるIPを検知し、確認すると、そのIPアドレスを次の更新サイクルで、ファイアウォールに送信しますので、ゼロディ攻撃からユーザを保護することができます。

●ボットネットの「コールホーム」をブロック
ThreatSTOPを使用するファイアウォールは、ボットネットおよび犯罪マルウェアの加害者として知られている脅威リスト上のIPアドレスとの間ですべてのトラフィックをブロックします

●ネットワークパフォーマンスを向上させ、帯域幅の使用率を削減
ThreatSTOPを使用するファイアウォールは、不正なトラフィックをフィルタリングしますので、ネットワークサーバおよびセキュリティインフラストラクチャの負荷は削減され、帯域幅はより効率的に使用されます

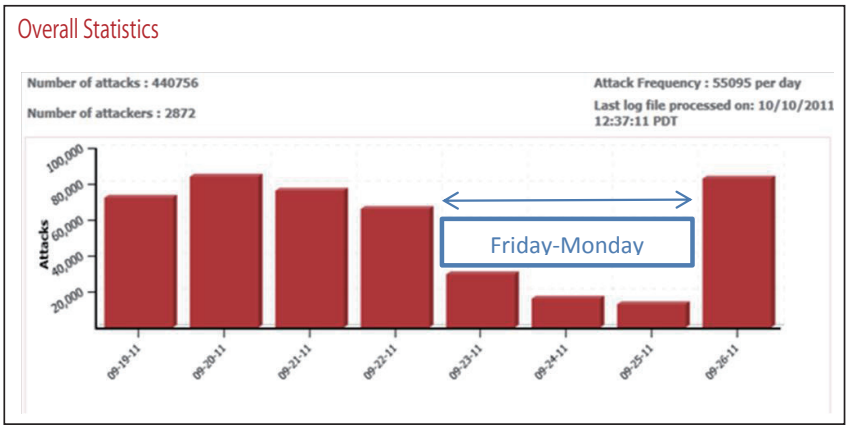
●スパムや攻撃のリスクを削減
ThreatSTOPを使用しているファイアウォールは、脅威となるIPアドレスからの着信パケットを見ると、すぐにそれを拒否します。つまり、送信者に対して該当ネットワークはインターネットから「消えて」いるような効果が生まれ、攻撃対象からはずされます。

●他のセキュリティ機器/サービスとの連携
・SIEMやIDSで検知したIPアドレスをWeb UIやAPIを介してThreatSTOPのカスタムリストに追加することも可能
・ThreatSTOPはIPスキャンをブロックしますので、Imperva クラウド WAF (Incapsula) サービスを補完

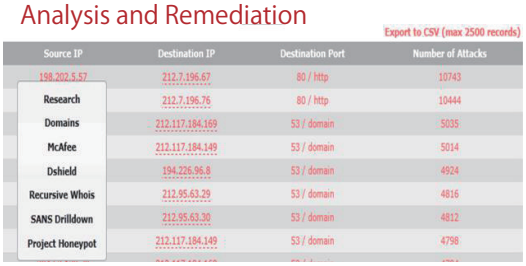
サポート機器

◆Fortinet FortiGate　◆Palo Alto
◆Juniper SRX　◆Cisco ASA　◆Vyatta　◆CheckPoint

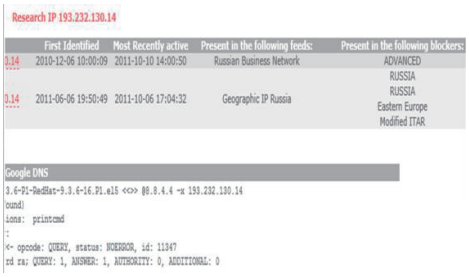
Webベースのレポート例



Analysis and Remediation



Forensics Drill Down



NVC NETWORK VALUE COMPONENTS

株式会社ネットワークバリューコンポネンツ

〒144-0035 東京都大田区南蒲田2-16-2
電話: 03-5714-2050　http://www.nvc.co.jp/

(threatstop_v2_B51)