ホワイトペーパー

脅威インテリジェンスでインシデント対応を加速する

ケーススタディ提供元：

目次

脅威インテリジェンスによるインシデント対応の改善

そこは過酷な世界である。国家支援アクターが強力な新しい機能を開発したとしても、犯罪グループは以前は国家だけが持っていた機能すら開発しおえている。攻撃者は、オンラインプロファイルとソーシャルエンジニアリングを通じて、標的に関する詳細な書類を作成し、その情報を使ってスピアフィッシングメールを作成できる。組織のシステムへの足がかりを得てからデータを盗み出すまで、わずか数日ということもある。

ベライゾン社の2016年のデータ侵害調査レポートによると、ほとんどのサイバー攻撃は検出されず、4件に1件よりも少ない。これを主な理由の1つとして、組織はインシデント対応チームとコンピュータ緊急対応チーム（CERT）に、攻撃の検出と無効化をより迅速かつ効果的に行うよう圧力をかけている。攻撃者が組織のシステムを危険にさらすまでにわずか数分しかかからないならば、データの漏えい防止のために、インシデント対応チームができるだけ早く効果を出せなければならない。

この重要な数日間で多くのことが起こり得る。にもかかわらず、組織やそのセキュリティオペレーションセンター（SOC）が焦点の置き所を間違えると、機会を逃す可能性がある。組織が効果的にサイバー脅威と戦うには、脅威インテリジェンスが重要な役割を果たす次の2つの重要な領域で、応答時間を加速する必要がある。

1. **迅速なエスカレーション**：深刻なサイバー脅威をインシデント対応チームにエスカレーションするスピード
2. **迅速な反応**：インシデント対応チームがサイバー脅威を無害化するスピード

1 迅速なエスカレーション

多くの重大なインシデントがインシデント対応チームに報告されない。その背景にあるのは、サイバー脅威への最初の対応が、通常の運用を維持することを主な関心事とするシステム管理者に任されているということである。たとえば、シスアドが、悪意のあるソフトウェア（
例：パスワードを盗むキーストロークロガー）がデスクトップPCで見つかったと知っても、そのソフトウェアを削除する際にウイルス対策ソフトウェアの有効性を信頼している場合がある。慎重なシスアドであれば、影響を受けるマシンをシステムイメージから再インストールするという追加手順を実行するかもしれない。

しかし、こうした基本的なアプローチも、次のような重要性を秘めた事実を見逃している。マルウェアはどのようにしてシステムに侵入したか？誰がそこに置いたか？同時に起こっている他の脅威はないか？何か危険なことが起こっているか、または起こりそうか？ステータスランプを「緑」に戻すだけでは、サイバー脅威と戦うのに不十分である。

インシデント対応チームにサイバー脅威のエスカレーションをいつ行うのが正しいか、シスアドにはわかりにくい。アラートや侵入の試みが多すぎて、役に立たない情報に隠れてしまうのだ。セキュリティベンダーは、IPアドレス、コンテキスト不足、品質評価、または有効期限の長いリストなど、生データを提供することが多い。

そしてこれらが非常に多くの誤検知をもたらす。

実用的な情報にするには、組織は低レベルの脅威と高レベルの脅威を見分ける必要がある。これが脅威インテリジェンスの重要なアプリケーションとなる。サイバー脅威に関する情報をシスアドのダッシュボードに組み込めば、攻撃されたときにアラームをオフにするだけでなく、いつエスカレーションをするべきかシスアドにわかるようになる。

2 迅速な反応

インシデント対応チームが組織に到着しても、効果的なリアルタイムの対応を開始するまでに数時間、長くて数日を要する。チームには次のような進める責任がある。悪意のある実行可能ファイルはどのように導入されたか？どのマシンから？いつ？次のステップを防げるか？いまだに、インシデント対応チームの多くの重点事項を、デジタルフォレンジックに依存しすぎている場合が多い。そのため、数週間から数か月を要する。

データフォレンジックの背後にある考え方は、犯人特定のためだけでなく、法廷で有罪判決を得るための十分なエビデンスを収集することである。この後は、犯罪捜査の他の分野での法執行アプローチに従う。そのためには、専門業者が感染したマシンをオフラインにして、
ストレージメディアのコピーを作成し、感染したファイルとコンピューティング環境の間の相互作用を分析する必要がある。これらを行う間、常にフォレンジックアクティビティの監査可能な記録を維持しておく。

このような複雑さのため、データフォレンジックは困難な作業である。デジタルフォレンジックを実施するには時間とリソースに多大な投資が必要であり、うまくいけば捜査官が数週間または数か月以内に、犯罪を報告するのに十分なエビデンスを法執行機関に提出できる。
その上、見込まれる報酬は高くない。外国の敵対者を逮捕したり、断罪したりすることは非常に難しいので、サイバー犯罪は地元の警察署にとって最優先事項とならない。

そのため、インシデント対応チームは、エビデンスの完全な保存ではなく、効果的な防御のスピードを重視する迅速なアプローチに移行している。

脅威インテリジェンスを使用すると、インシデント対応チームは、接続デバイスのゼロデイ攻撃から電子メールを使った有名なフィッシング攻撃に至るまで、あらゆる情報の膨大なソースを利用できる。対応側は、PCハードウェアの分析やコードサンプルの分解に時間を費やす代わりに、まず脅威インテリジェンスの統合フィードを検索して一致するものを見つけるべきである。

脅威インテリジェンスとインシデント対応を組み合わせると、組織は脅威をより速く検出し、あまり中断せずに攻撃を抑え、十分な速さで対応できるようになるため、攻撃者によるデータ盗難や、その他の持続的損害を防止できる。

図1：全体的な脅威の状況に関する洞察–ベライゾン社データ侵害調査レポート

インシデント対応への脅威インテリジェンス追加

次の4つのコンポーネントを使用して、インシデント対応に脅威インテリジェンスを追加する。

1 インテリジェンス要件

脅威インテリジェンスの出発点は、次のような質問への回答をまとめることで、ニーズを理解することである。

- 業界と事業にかかわる最大のリスクは何か？
- 組織を狙いそうな攻撃者はどんなタイプか？
- 攻撃者にとって最も価値のあるデータとプロセスは何か？

サイバーセキュリティ専門業者の支援を受けて組織のインテリジェンス要件を監査することにより、防御のために最善の準備が必要な攻撃のカテゴリーを総合的に把握できる。

2 脅威インテリジェンスフィード

インテリジェンス要件の調査をもとに行う次のステップは、最も可能性の高い脅威に対処できるインテリジェンスフィードを見つけることである。

たとえば、最大のリスクが研究開発プロジェクトの産業スパイである場合、注目すべきは、政府機関への従事がわかっている事業体が使用するマルウェア専門のフィードである。

同時に、情報共有・分析センター（ISAC）や業界固有の他のコミュニティが提供する脅威インテリジェンスにも接続すべきである。

複数のフィードによって配信される情報は重複している可能性がある。これは想定内でのことで、複数のソースからのデータをクロスチェックできるメリットがある。適切なツールを使えば、重複データを簡単に処理できる。

3 脅威インテリジェンスプラットフォーム

サイバー脅威防御が未成熟な組織は、脅威インテリジェンスフィードからの生データに依存しすぎていることが多い。さまざまなフィードを取り込んで利用できる適切なツールがなければ、フィードは使いにくい。あまり使わないフィードに含まれた重要な事柄を見逃したり、日々のデータ豊富なフィードからの情報に圧倒されたりもするだろう。フィードを並べ替えて処理する作業でも、企業のIT部門にとってかなりの負担となり得る。

脅威インテリジェンスプラットフォームは、内外のフィードを含むさまざまなソースからのインテリジェンス統合を自動化する。システム管理者とインシデント対応チームは、最新の脅威情報を1つの検索可能な場所に配置することで、脅威インテリジェンスのさまざまなソースが提供する広範なデータを最大限に活用できる。

4 プロセスと役割

システム管理者は脅威インテリジェンスを使用して、インシデント対応チームを呼び出すべきサイバー攻撃を適宜発見できるようになる。インシデント対応チームは脅威インテリジェンスを使用することで、少ない労力で速く結果を得られる。脅威アナリストは脅威インテリジェンスの使用によって、組織のサイバーリスクに対する全体的な姿勢を継続的に調整できる。

システム管理者：企業向けの脅威インテリジェンスプラットフォームは、企業のセキュリティテクノロジーと統合されており、プラットフォーム内のシステム管理者と、そこですでに使われている診断ツールに豊富なデータを提供する。システム管理者は、サイバー攻撃の検出を確認するだけでなく、攻撃者に関する情報を発見して、必要に応じてインシデント対応チームに電話するという判断を妥当とみなすことができる。

インシデント対応チーム：インシデント対応チームは、脅威インテリジェンスプラットフォームに含まれるすべてのフィードに直接働きかけて、いくつの主な特性に基づいてでも検索できる。さらに、脅威インテリジェンスと企業ITソリューションの統合により、内部データソースとシステムの内容がわかりやすくなり、インシデント対応チームがサイバー脅威に迅速に対応できるようになる。

脅威アナリスト：インシデント対応チームに大きく依存している組織でも、内部脅威アナリストが果たす役割は重要であり、脅威インテリジェンスプラットフォームに取り込まれるフィードを、組織で発展するリスクプロファイルに確実に一致させるように努める。継続的な役割として、脅威アナリストは業界の同業者と協力し、新たな脅威に関する情報を常に入手もして、受け取った情報に基づいて組織の脆弱性の評価もしなければならない。

インシデント対応による脅威インテリジェンスの組織上のメリット

1 迅速なインシデント対応

サイバー防御の専門家は、デジタルフォレンジックの引き出しプロセスを開始する代わりに、サイバー攻撃への正しい対応の考案に集中できる。攻撃者と攻撃方法に関するタイムリーで完全な情報に基づいて、違反を修復する。

2 損傷と損失の制御

脅威インテリジェンスは、インシデント対応チームの能力を向上させ、ユーザー権限の取得、監視ソフトウェアのインストール、データの盗用など、攻撃者が最終目標を達成するのを防ぐ。

3 自動化によるコスト削減

脅威インテリジェンスを既存のITセキュリティソリューションおよびシステム管理ツールに接続する（例：IPアドレスブラックリストを毎日更新するプロキシサーバーの更新）ことにより、組織はサイバー攻撃者の攻撃機会を狭めるだけでなく、システムのダウンタイムを減らし、より生産的な活動のためにITリソースを解放する。

ケーススタディ：フォレンジックよりも速く

疑わしい電子メールの受信者がその内容と信頼性について送信者に質問したとき、大企業での潜在的なサイバー脅威に関する警告が発せられた。Fox-ITのコンピュータ緊急対応チーム（FoxCERT）が顧客の現場に到着し、社員のマシンがマルウェアに感染していること、被害者のアドレス帳に名前のある全員に電子メールを送信していたことがわかった。

このような状況での通常の対応は、従来のフォレンジック調査を開始することである。調査員が感染したマシンを調べて悪意のあるコードサンプルを探す。次に、専門業者は悪意のあるコードと考えられるものを保護されたサンドボックス環境に配置し、動作を観察し、必要に応じてリバースエンジニアリングしてその機能を判断する。このようなプロセスは、悪意のあるコードの複雑さによっては数日以上かかる場合もある。

このケースでは、Fox-ITはもっと高速で効果的なアプローチを採用した。FoxCERTは、感染したコードのサンプルにハッシュ関数を適用することでそのマルウェア固有の「シグネチャ」を捕え、EclecticIQプラットフォーム内でそのシグネチャを確認した。マルウェアがどのように働き、マルウェアにどんな機能があるかをEclecticIQプラットフォームから学び、すぐに一致するものを見つけた。
これにより、被害者のマシンに自己インストールした後のマルウェアが、アドレス帳に基づいて他のユーザーに電子メールを送信することにより、自分自身をばらまいていることが明らかになった。

EclecticIQプラットフォームは、マルウェアがリモートコントロールとキーロガー機能を備えていることも示した。また、診断を確認してマルウェアを削除する方法も提示した。対応チームは、その組織内のマシンで他の侵害の痕跡がないか確認し、多くのマシンが同じマルウェアに感染していることを明らかにした。FoxCERTは短期間で、組織全体の感染したコンピュータを一掃した。

さらに、EclecticIQプラットフォームの脅威インテリジェンスは、攻撃に対する視野を広げた。このマルウェアは、既知のマルウェアファミリーの一部であり、インテリジェンスコミュニティで広く活動を追跡されていた外国グループに属する可能性のある幅広いキャンペーンの一部だった。この知識をもとに、インシデント対応チームは、この攻撃が顧客を標的にしただけでなく、より広い活動範囲の一部であったことを顧客に通知することもできた。

重要ポイント：フォレンジック調査は、特に新しい攻撃タイプとコードサンプルが発見された場合、サイバー防御において引き続き非常に重要な役割を果たす。それでも、サイバー防御共有コミュニティ間ですでに検出、分析、および配布されているコードサンプルに対してフォレンジック分析を実行することは、時間とリソースの大きな浪費となる。

脅威インテリジェンスを利用したインシデント対応は、環境内の（他の）脅威を無効化して見つける最速かつ最も効果的な方法を提示する。

さらに、脅威インテリジェンスを使用して敵対者の他の攻撃モードを特定することにより、インシデント対応チームは顧客保護のための徹底した任務を遂行できる。

ケーススタディ：攻撃者の*手口*を理解する

ある会社の幹部が、母親からの、疑わしい添付ファイルを含むとされる電子メールを受け取った。電子メールは不正であると検出され、Fox-ITのCERTチームに転送された。

そこでFoxCERTチームは、電子メール、添付ファイル、および添付ファイルの一部である感染したペイロードを詳細に分析した。この分析から、次のようなデータポイントが得られた。電子メールの件名、添付ファイルのファイル名（MS Word文書）、電子メールの送信に使われたIPアドレス、「差出人」アドレスとして使われたドメイン名、ペイロードの意図的な動作（たとえば、IPアドレスまたはドメインへの発信接続の試行）、およびペイロードの一意のハッシュである。

次に、FoxCERTチームはこれらのデータポイントをEclecticIQプラットフォームに供給した。その結果、「スピアフィッシング」メールをターゲットに送信する攻撃方法を好む既知の脅威アクターに関する情報が明らかとなった。脅威アクターの手口は、異なるファイル名を使って、感染した添付ファイルを送信することだった。プラットフォームには、同じ脅威アクターによる他の攻撃で見られた他のファイル名が保存されていた。

そのインテリジェンスを念頭に、FoxCERTチームは電子メールログでこれらの疑わしいファイル名を検索した。そうすることで、他の社員、つまり同じ脅威アクターから添付ファイルを開いた可能性のある、他の企業幹部への他の「スピアフィッシング」メールを特定した。FoxCERTチームは、他のファイル名の電子メールを受信した他の社員のマシンを調査したが、電子メールを開いた痕跡は見つからなかった。

重要ポイント：脅威インテリジェンスを使ってキャンペーンのソースを特定することにより、インシデント対応チームは、元の電子メールだけでなく、同じ敵対者からの他のスピアフィッシング電子メールについても、修復への最も直接的な道をたどった。

このアプローチにより、インシデント対応チームは、ネットワーク全体で全社的なインシデント対応検索を行う必要性を避け、最終的にコストを削減して時間を節約した。

結論

サイバー攻撃の最初の重要な数時間や数日間、重点の置き所を間違えると、組織はデータや経済的損失を防ぐ機会を逃してしまう。

深刻な脅威をできるだけ早く検出すると、迅速なエスカレーションにつながり、対応も早くなる。脅威インテリジェンスとインシデント対応を組み合わせると、組織は脅威をより速く検出し、あまり中断せずに攻撃を抑え、十分な速さで対応できるようになるため、攻撃者によるデータ盗難や、その他の持続的損害を防止できる。

緊急事態対応機能に脅威インテリジェンスを追加しようとしている組織は、最初にインテリジェンス要件の範囲を明らかにするべきである。これらの要件に基づいて、次のステップでは、関連するインテリジェンスフィードとオープンソースインテリジェンスデータを選択して取得する。その後、攻撃中にそのデータを有効にするには、他のITセキュリティソリューションや外部パートナーに接続する脅威インテリジェンスプラットフォーム内で、インテリジェンスフィードを取り込み、正規化し、分析することが不可欠となる。

このアプローチによって、組織はインシデントに迅速に対応でき、サイバー攻撃によって引き起こされる経済的および評判上の損害を減らすことができる。さらに、プロセスを自動化し、インシデント対応に関連するコントロールを体系化することで、組織は脅威インテリジェンスの複雑さを管理するための非構造化で手動のアプローチと比較して、大幅にコストを削減し、効率性を獲得することができた。

EclecticIQは、大企業、政府、MSSPと協力して、サイバー脅威の検出、防止、対応を改善します。

EclecticIQのアナリスト中心の脅威インテリジェンスプラットフォームであるEclecticIQプラットフォームは、脅威インテリジェンスの実践とインテリジェンス主導のSOCおよびCERT運用の有効性を高めます。EclecticIQプラットフォームは、さまざまなソースからインテリジェンスを自動的に収集します。共同の内部ワークフローを可能にします。また、企業のセキュリティテクノロジーと統合し、外部の情報共有コミュニティとの安全な交換をサポートします。

弊社は、EU IPACSOのサイバーセキュリティ賞、および「最も破壊的なイノベータ」としてデロイトのテクノロジーFAST50ライジングスター賞を受賞しました。

EclecticIQは、OASIS CTI TCのメンバーであり、FS-ISACのアフィリエイトメンバーです。

EclecticIQは、オランダのアムステルダムに本社を置いています。

EclecticIQの詳細については、www.eclecticiq.comをご覧ください。

販売や製品のデモについては、sales@eclecticiq.comにお問い合わせください。または、電話+ 31（0）20 737 1063におかけください。

Twitterは@eclecticiqをフォローしてください。