事業会社自身で脅威インテリジェンスを活用するために

目次

前置き

セキュリティベンダーではなく、あくまで事業会社自身で脅威インテリジェンスを活用、運用するための問題と解決策のTipsをまとめていきます。
基本的に`Tactical level`を主としたインテリジェンスを扱うことを主軸として書きます。

また、お金をかければ解決できそうな問題もあったりしますが、自社に合ったインテリジェンスや自社で観測したインテリジェンスを活用するとなると、事業会社である程度のインテリジェンス運用していくことが必要なので、ベンダと連携はしつつもあくまで自社でインテリジェンス運用していることを前提とします。

Tips

リソース問題（モノ）に対するアプローチ

日々脅威インテリジェンスを収拾すると、自動化している場合大量のインテリジェンスを日々収拾することになります。
自社でこの仕組みを長期運用していると以下の問題が顕在化してくるかもしれません。

- 収集したインテリジェンスのストレージ問題

  長期間インテリジェンスを収集していると、そのインテリジェンスをどう保持していくのか問題が出てきます。

> TIP「1万/dayを越えるインジケータが登録されるなんて無理です！」
> ぼくたち「た...耐えてくれ...」
>
> ...数年後
> TIP「ぐわー！（爆散）」

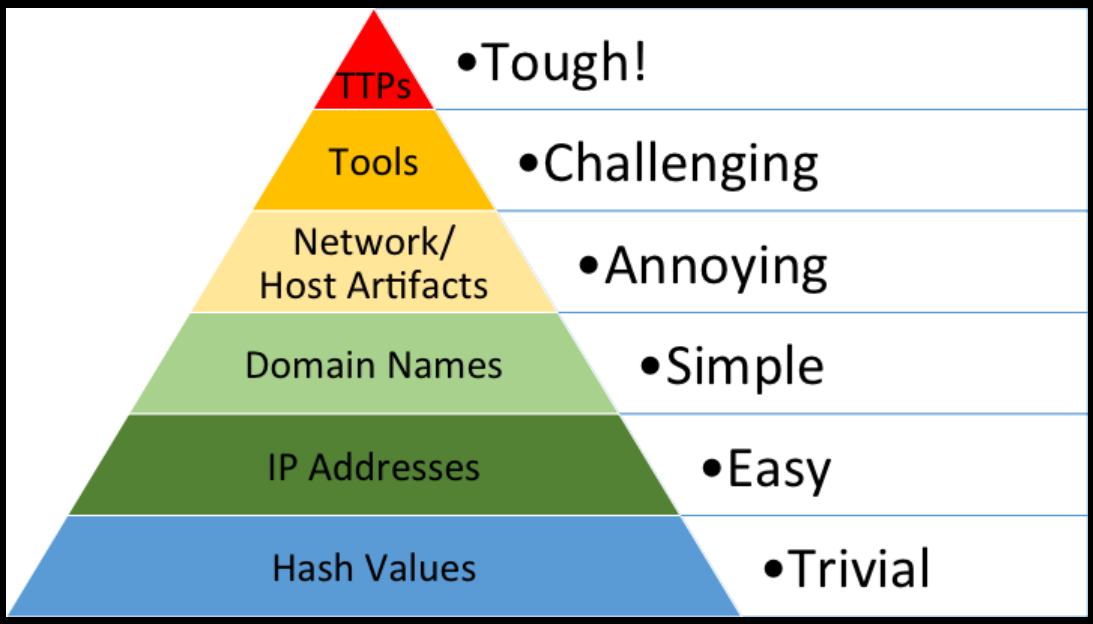
  解決策としては、以下のようなものがあります。

1. 金銭的解決（大容量）
2. 定期的にインテリジェンスを削減

  基本的に1ではどこかで限界が来るので、2のアプローチを取ることになるかと思います。
  ここでどう削減していくかのアプローチを記載します。

Pyramid of Pain

以下の図を見たことがあるかもしれません。



詳しくは`Pyramid of Pain`などで調べていただければと思いますが、簡単に説明すると、ピラミッドの下段になればなるほど、変更が簡易で、上段になればなるほど変更が難

しいということを示しています。
HashやIPなどは攻撃者にとって変更が容易なため、インテリジェンスとして利用価値があるタイミングは限られています（C2アドレスは直ぐに変更されるし、キャンペーンが過ぎれば数日でオフラインになります）。
Toolの情報は攻撃者側のMalware作成やオペレーションの修練もあるため変更が難しかったり、また脅威アクターが狙う初期アクセス方法（公開RDPでの侵入など）は企業の流行などもあるため、変更されないことが多いです。

解決方針

上記のPyramid of Painを元に、インテリジェンスの削減方針を考えることができます。
例えば、IPやHashなどのインテリジェンスは、攻撃者が変更することが容易なため、これらの情報から定期的にリソースを削除していくことが考えられます。
APTのレポートなど、ピラミッドの上位に位置する攻撃手法などが乗っているレポートなどは、攻撃者が変更することが難しいため、長期間保持しておく方針がよいと思います。

Detect or Blockに対するアプローチ

インテリジェンス活用として、そのインテリジェンスに合致する通信やファイル作成などをブロックするのか検知に留めるか問題があります。

事業会社であれば、そのサービスの性質上ブロックを行うと以下のような事が発生する可能性があります。

> ぼくたち「よっしゃ！Blockじゃ！」
> お客様「あれ、oo社のサービスへアクセスできない！」
> 社員「このサイトアクセスできない！業務が止まってしまう！」
>
> ぼくたち「うわー！問い合わせ地獄だ！」

PV数などが命のサービスであれば、自社サービスへのアクセスをブロックすると誤検知が発生した場合、致命的になったりしますね。

解決方針

ファイルHashやURLhausにある相当のURLフルパスであればBlockでもいいとは思いますが、IPなどはいくら攻撃者が利用しているといっても誤検知が出てきます（クラウドインフラとか特に）。なので基本的な方針としては検知に留める方針が良いかと思います。
イメージとしては「普段の検知ルールでも引っかからない場合に、検知網を広げるために利用する」といった形です。
TIをあくまで取っ掛かりとして利用するイメージですね。

Tactical levelとしてお話しましたが、Operational levelやStrategic levelのインテリジェンスも同様に考えることができるかと思います。あくまで取っ掛かりであり、どう扱うかは会社毎に当てはめて吟味する必要がある。

最後に

さらっと書いたのですが、インテリジェンスの利用を検討する前に、守るべき資産の把握や、通常の監視基盤の構築運用などをある程度整備した方がよいです。
あくまで、既存の仕組みを補うスパイスとして活用してもらえればと。

検知ruleに関しては、他にもインテリジェンスの活用観点があるので、また別の機会に書ければと思います。
鮮度の問題があるので。