導 入 事 例

Carbon Black.

NVC NETWORK VALUE COMPONENTS

TIS株式会社

過検知で従業員の生産性を妨げることなく未知の脅威に対処するため「Cb Response」を採用。マネージドセキュリティサービスとの組み合わせで運用負荷を下げ高い防御を実現

連日のように新たな脅威が登場する昨今、情報システム部門の負荷は高まるばかりだ。エンドポイントセキュリティ製品が発する誤検知・過検知は、その仕事をさらに過酷なものにしている。TIS株式会社ではこの課題を解決するため、米CarbonblackのEDR製品を採用。専門家の知見が得られるマネージドセキュリティサービスと組み合わせ、負荷を減らしつつ迅速な対応を実現している。

課題

- エンドポイント製品の過検知が多く、対応に当たる情報システム部門、エンドユーザー双方の負荷が高かった
- 複数のセキュリティ製品がバラバラに出力するログの統合管理が困難だった
- 24時間365日体制でのアラート対応が困難だった

成果

- Cb Responseの採用で、隔離をはじめとする対応までを円滑に行えるようになった
- Cb Responseとマネージドセキュリティサービスの連携で、何が起きているか一元把握が可能になった
- 機械だけに頼らず、Cb Responseから得られた情報と専門家の知見を生かした対応が可能になった

Profile

TIS
TIS INTEC Group

■TIS株式会社（TIS Inc.）
■設　立　2008年4月1日
■所在地　〒160-0023
東京都新宿区西新宿8丁目17番1号
■U R L　https://www.tis.co.jp/

TISは独立系のトータルシステムインテグレーターとして、金融、製造、流通、エネルギー、公共など、幅広い分野のシステム構築・運用を手がけてきました。インフラからアプリケーション、運用プラットフォームまでを提供し、長年にわたって培ってきた経験とIT技術を通じて、3000社を超えるお客様のビジネスを支えています。

未知のマルウェアを少ない手間で検出し、被害を抑えるためEDRを導入

グループで約2万人を擁するTISインテックグループの中核企業として、金融や製造、流通、公共など、あらゆる業種を対象に、システムインテグレーションのほか、データセンターやクラウドサービスといったITソリューションを開発、提供しているのがTISだ。近年ニーズが高まるセキュリティ分野のビジネスにもいち早く1999年から参入し、コンサルティングや診断も含めたサービスを提供している。

顧客に高品質のセキュリティソリューションを提供する裏付けとして、TIS社内の情報システムでは「万全な体制を取っています」と、TIS株式会社 管理本部 情報システム部エキスパートの音喜多 順氏は説明する。エンドポイントのセキュリティ製品はもちろん、インターネットとのゲートウェイではファイアウォールにフィルタリングソフトなど多層防御を実装し、既知のマルウェアを検出、排除できる体制を整えてきた。

一方で、課題も残っていた。検知に必要なシグネチャが用意されていない未知のマルウェアを、いかに少ない手間で、また誤検出を避けながら見つけ出し、被害を抑えるか――この目的を達成するためTISでは、同社のパートナーである米Trustwave社のマネージドセキュリティサービスとともに米CarbonblackのEndpoint Detection & Response（EDR）製品「Cb Response」を導入し、セキュリティのいっそうの強化を図っている。

TIS株式会社
管理本部
情報システム部エキスパート
音喜多 順 氏

TIS株式会社
管理本部
情報システム部長
入山 秀樹 氏

TIS株式会社
プラットフォームサービス本部
プラットフォームサービス事業部
エンタープライズセキュリティサービス部長
茂手木 隆文 氏

TIS株式会社
プラットフォームサービス本部
プラットフォームサービス事業部
エンタープライズセキュリティサービス部 副部長
諸田 陽宏 氏

万全のセキュリティ体制を敷くものの、アラート対応や過検知に課題

TIS情報システム部では、縦割りで専任の担当を置くのではなく、全メンバーが他の業務とクロスオーバーする形でセキュリティシステムを運用している。ただ、万全の体制を敷いたがゆえの課題があった。複数のセキュリティツールの管理コンソールが別々に動いており、ログを取得するタイミングもバラバラで、「今、何が起きているか」を一元的に把握するのが困難だったのだ。

またこの体制では、各セキュリティツールが発したアラートへの対応が、情報システム部に

とって大きな負荷となっていた。セキュリティインシデントは業務時間中にばかり発生する訳ではない。土日や深夜といったタイミングに発生したアラートを確認して対応を指示する負荷は無視できなかった。

その上、TISには、一般の企業とは少し異なる事情があった。多くの社員がソフトウェア開発に携わっているため、エンドポイントの環境が多種多様なのだ。物理のみならず仮想環境もあり、さまざまな開発用ツールをインストールするため、管理者権限での作業が不可欠な場面もある。TISでは標的型攻撃対策を狙ってエンドポイントセキュリティ製品も導入していたが、「誤検知、特に過検知が多いことが課題でした。アラートが出れば見ないわけにはいきませんが、大量に検出されると、重要なものがその中に紛れてしまう恐れがあります。一方で、ソフトウェア開発に必要なツールが対策ソフトの過検知で止められると、生産性の低下につながってしまいます」(音喜多氏)

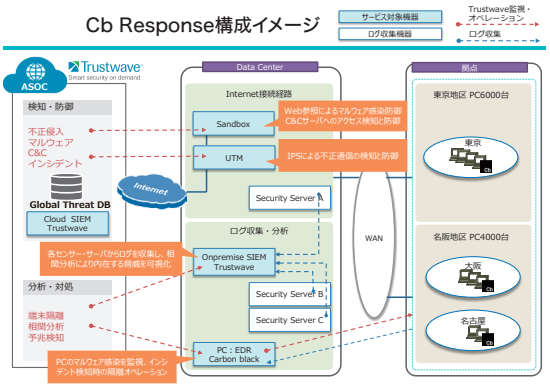
だからといって、誤検知を避けるために検出率を緩めるとマルウェアまでもがすり抜ける恐れがあり、何のためにエンドポイントセキュリティ製品を導入したのか分からない、本末転倒な状況に陥る。こうした経験を踏まえて音喜多氏は「機械に頼っていては無理で、やはり知見を持った専門家が必要だろうと考えました」と振り返る。

米Trustwaveのマネージドセキュリティサービスとの連携で「見つけたらMSSがタイムリーに遮断」を実現

そこで注目したのが、シンガポールテレコムの子会社で、TISがパートナーとなっている米Trustwaveのマネージドセキュリティサービス(MSS)だった。高度な知見を持った専門家が、さまざまな機器から収集したログをSIEMで統合解析し、本当に深刻な兆候があれば通知してくれる。情報システム部が24時間365日体制で気を張りつめなくてもいい。

残る問題はエンドポイントをどのように監視し、情報を収集するかだが、実はTrustwave MSSが対応していたEDR製品の一つがCb Response であり、検知のプロにとっても使い慣れているツールだった。他のEDR製品も検討したというが、「『マルウェアを見つけたらタイムリーに当該端末を遮断したい』という厳しい要件を唯一満たしたのが、Trustwave MSSとCb Responseの組み合わせでした」(TIS株式会社 プラットフォームサービス本部 プラットフォームサービス事業部 エンタープライズセキュリティサービス部長 茂手木隆文氏)

Cb Response構成イメージ



こうして2017年夏からトライアル導入を開始したが、同エンタープライズセキュリティサービス部 副部長の諸田陽宏氏は、「使う側からすると、導入されていることに気付かないくらい軽く動作しました。また、PCに導入していたいろいろなシステムやツールとも競合せず『仲良く』動きました」と感想を述べる。

一方管理者の視点からは、「非常に多機能で、リアルタイムに詳細な情報を取得できる点に驚いています。過去、誤検知が発生しても理由が分からず、ベンダーとやり取りしても不明瞭で利用者からの問い合わせに応えられず時間ばかり費やしていたのが、Cb ResponseではPCの中の振る舞いが手に取るように分かるようになりました」(音喜多氏)という。

音喜多氏はさらに、「EDRなしのセキュリティがオートマ車だとしたら、Cb Responseはマニュアル車。さまざまなメーター類が充実しており、見る知識を持ったプロが使えば『鬼に金棒』で、非常に高い性能を発揮できると思います」と述べている。

全社に展開、その知見を活用して顧客向けにもソリューションを展開

こうした効果を見込みTISでは、ネットワークバリューコンポネンツ(NVC)の支援も得ながらCb Responseの導入作業を進めている。「あらかじめTrustwave MSSとの組み合わせ用の推奨設定を提供いただいたほか、製品知識が豊富で安心して導入作業を進められました。特にフットワークが軽く、リクエストに対する回答が本当に早いのには助かっています」と諸田氏は評価する。2017年度中にTIS全社、約1万台に導入し、その結果を踏まえてグループ企業にも展開していく計画だ。

同時にTISではこの導入経験を生かし、Trustwave MSSとCb Responseを組み合わせたセキュリティソリューションを顧客向けに展開していく。PCI DSS対応で北米一の実績を持ち、世界9カ所に設置されたSOCが連携して脅威に関する動向をいち早くつかんでいるTrustwave MSSの知見と、Cb Responseから得られるあらゆるアクティビティの可視化、TISのエンジニアの知見を組み合わせることで、顧客のニーズに応えていく。

諸田氏はさらに、「エンドポイントセキュリティ製品ではいかに検知するかにばかり目が行きがちですが、検知した後は、何がしかの対応をしなくてはなりません。Trustwave MSSとCb Responseの組み合わせでは、自動的に端末のネットワーク遮断までできるため、IT担当者の負荷を大きく下げられますし、専門家の知見を踏まえて緊急度の高いインシデント防止にも役立ち、多くの企業が抱える『専門家が足りない』という悩みを解消します」と述べています。

TIS株式会社 管理本部 情報システム部長 入山秀樹氏は「折しも2020年の東京オリンピック・パラリンピックに向け、日本をターゲットにした攻撃の増加が懸念されます。標的型攻撃はもちろん、それ以外にも新たな攻撃が出てくるでしょう。自社が直接被害を受けないようにするだけでなく、踏み台とならないよう広い対策が必要です。そのためにTISでは総合力でニーズに対応していきます」と意気込みを見せています。

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/