お客様事例 › マルウェア対策

EDRでセキュリティ対策を行う スカパー・カスタマーリレーションズ

事例のポイント

導入の概要

- 企業におけるサイバーセキュリティ対策として注目されているのが、侵入後の検知・対応・復旧を行う「EDR」です。EDRの重要性を実感し、Cybereasonの導入に至った事例を紹介します。

ポイント

- EDRでセキュリティ対策を行うスカパー・カスタマーリレーションズ
- サイバー攻撃の高度化に備えてEDRに着目
- 優れたGUIと充実のSOCサービスが決め手
- 「侵入されたかどうか」が明確にわかることの安心感は大きい
- 自社のエンジニアリソースをコア業務に集中
- 優先順位をつけて対策を進めるべき

導入ソリューション

Cybereason EDR

侵入後の攻撃を振る舞いで検知する 次世代エンドポイントセキュリティ「EDR」

EDRでセキュリティ対策を行う スカパー・カスタマーリレーションズ

サイバー攻撃は、高度化・複雑化しています。これまで企業におけるサイバーセキュリティ対策といえば、アンチウイルスソフトやファイアウォールなどの導入が一般的でしたが、今やそうした既存の侵入前対策だけでは、サイバー攻撃を100%防ぐことは困難になっています。

そこで、次世代のサイバーセキュリティ対策として注目されているのが、侵入後の検知・対応・復旧を行う「EDR（Endpoint Detection and Response）」です。

そんなEDRの重要性を実感し、SCSKが提供するEDRソリューション「Cybereason（サイバーリーズン）」を1,250台の端末にご導入いただいているのが、コンタクトセンター運営、事務・バックオフィス業務運営、コンサルティングサービスを提供する株式会社スカパー・カスタマーリレーションズです。

同社はなぜEDRに着目し、Cybereasonの導入に至ったのか。同社が考えるこれからのサイバーセキュリティ対策について、スカパー・カスタマーリレーションズ、取締役兼 CISOの前田吉徳氏（以下、前田氏）、DX推進部テクノロジー推進チームマネージャーの大山裕宗氏（以下、大山氏）、DX推進部テクノロジー推進チームの繁倉崇宏氏（以下、繁倉氏）に、お話を伺いました。

サイバー攻撃の高度化に備えて EDRに着目

――スカパー・カスタマーリレーションズの事業についてご紹介をお願いします。

前田氏：弊社はスカパー JSATのグループ企業で、主に衛星放送の「スカパー!」を視聴するお客様を対象としたコンタクトセンター（コールセンター）などのBPO（Business Process Outsourcing）事業を行っています。また、「スカパー!」以外では、約40社の企業様のコンタクトセンターやBPOもご委託いただいており、年間でのコール数は着信400万件以上発信100万件以上、ブース数800以上と、コンタクトセンター事業としてはそれなりの規模です。そのほかに、事務・バックオフィス業務運営や、コンサルティングサービスも提供しています。

――なぜ、EDRに着目されたのでしょうか?

前田氏：EDRは、近年特に注目されているサイバーセキュリティ対策です。これまでは、マルウェアを検知して侵入そのものを防ぐEPP（Endpoint Protection Platform）というセキュリティ対策が主流でしたが、今やそれだけでは防ぎきれないほど、サイバー攻撃は高度化しています。

もちろん、EPPによる入り口対策は継続すべきですが、EPPだけでは侵入後の対策が後手に回るので十分とはいえません。ですから、これからのサイバーセキュリティは、侵入されることも視野に入れた「ゼロトラスト的な」考え方が重要と考えています。つまり、入り口

cybereason

お客様プロフィール

SPCC

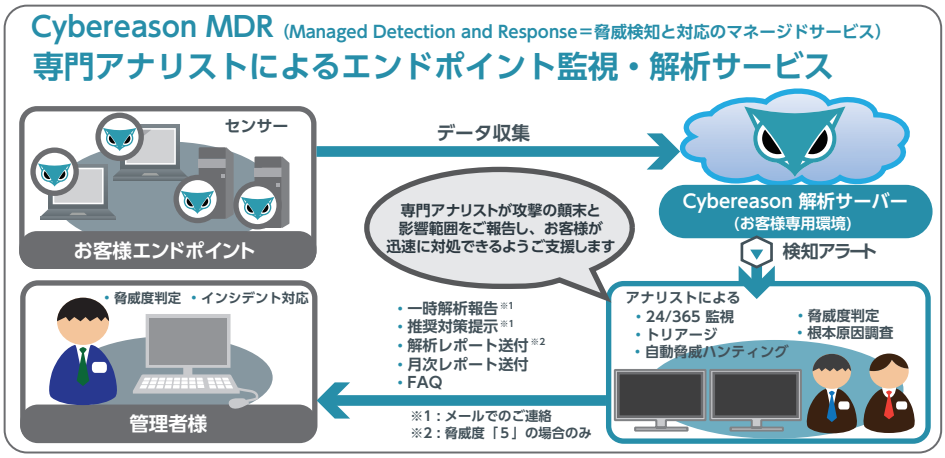
社　　名：株式会社スカパー・カスタマーリレーションズ
本社所在地：東京都品川区
設　　立：2000年8月
資 本 金：1億円
従業員数：450名（2021年3月現在）
事業概要：有料多チャンネル放送「スカパー！」のカスタマーセンター運営
U　R　L：https://www.spcc-sp.com/

株式会社スカパー・カスタマーリレーションズ
取締役兼CISO
前田 吉徳 氏

株式会社スカパー・カスタマーリレーションズ
DX推進部 テクノロジー推進チーム
大山 裕宗 氏

株式会社スカパー・カスタマーリレーションズ
DX推進部 テクノロジー推進チーム
繁倉 崇宏 氏

株式会社スカパー・カスタマーリレーションズ 様



だけではなく、EDRによる複数のセキュリティ対策を施す、「多層防御」を徹底する必要があるのです。

――スカパー・カスタマーリレーションズが、EDRの導入を検討された経緯を具体的に教えてください。

前田氏：EDRを検討し始めたのは2020年頃です。これまで弊社ではサイバー攻撃による被害が発生したことはなかったのですが、サイバー攻撃そのものは増加していたこともあり、セキュリティ対策を強化する必要性を感じていました。とりわけ、弊社は事業の特性上、非常に多くの個人情報を取り扱います。ですから、事業の継続性に影響を及ぼすセキュリティインシデントは絶対に避けなければなりません。
私は以前、コンピューター犯罪の調査などを行う「デジタル・フォレンジック」にも多少関わったことがあり、サイバーセキュリティに関しては様々な経験を積んできました。そうした経験から大事にしているのは、「現状のセキュリティ対策に満足してはいけない」「入口対策だけでは不十分。侵入された場合を考え、各攻撃段階を意識した手を準備する」という考えです。そこで、弊社としてどのようなセキュリティを行うべきか、DX推進部とともに検討することにしました。
大山氏：要請を受けたDX推進部では、まずセキュリティ対策をさらに強化するための調査を行いました。その過程で知ったのが、「多層防御」やセキュリティ対策を信用しない「ゼロトラスト的考え方」、そして「EDR」の3つでした。私は、「侵入を素早く検知・対応して被害を最小限に抑える」というEDRの思想に共感し、前田と検討を重ねた結果、全社に導入することを決めました。

優れたGUIと充実のSOCサービスが決め手

――さまざまなEDRソリューションがある中で、Cybereasonを選んだ決め手は何だったのでしょうか?

大山氏：機能はもちろん、知名度やシェアなども考慮して、4製品程をピックアップしました。
その中からCybereasonを選んだ理由は、まず情報を提示したり操作を受けつけたりするGUI（グラフィカル・ユーザー・インターフェース）が最も優れていたことです。
また、サイバーリーズン・ジャパン株式会社が提供している、SOC（セキュリティオペレーションセンター）サービスが充実していたことも評価しました。我々に代わってエンドポイントを監視し、リスクを検知したら「報告」を行い「対策」を提示してくれるので、SOCサービスがあることは非常にありがたいと感じたのです。最終的に導入や運用に要するコストも含めて検討し、Cybereasonが総合的に優れていると判断して決めました。

――Cybereasonの導入をどのように進めていったのでしょう。

大山氏：SCSKさんに問い合わせを行い、弊社のシステムでセキュリティ対策が正しく機能するか概念実証（PoC）を行い、問題がないことを確認してから導入しました。導入を進める上で注力したのは、運用体制の構築です。
まず、実際にサイバー攻撃などのインシデントが発生した場合、SOCサービスから報告を受けます。その後はどのような連絡体制で、誰がどう判断し、どう動くのか。細かい点も含めて事前にしっかり体制を構築しました。体制を構築しない場合、迅速に動くことができず、EDRを導入した意味がなくなってしまうと考えたからです。Cybereasonをただ導入して終わりというのではなく、きちんと運用に落とし込むことが大切だと考えました。
前田氏：運用に落とし込むことの大切さは、弊社の事業にも根付いています。コンタクトセンター事業では、非常に多くのお客様とやりとりが発生するため、CSR（Customer Service Representative：お客様応対オペレーターの名称）一人ひとりのノウハウに任せてしまうのはリスクが大きいのです。
そこで重要なのが、どこまでマニュアル化できるのかということです。途中でオペレーターが代わっても、対応が変わってはいけません。誰かが会社を休んでも、辞めても、業務が滞らないような体制が必要なのです。

――導入決定から運用を開始されるまで、どれくらいかかりましたか?

繁倉氏：EDRの検討を始めてから体制構築まで入れても、約2ヵ月です。SCSKさんのサポートもありましたので、運用自体は1ヵ月もかからないくらいでスタートできました。

「侵入されたかどうか」が明確にわかることの安心感は大きい

―― Cybereasonを導入した効果について、どう感じていますか?

繁倉氏：一番の効果は、「侵入されたかどうか」を、迅速かつ明確に判明できることです。Cybereasonがなければ侵入や活動に気づくまで時間がかかりますし、その間にほかの端末も感染してしまうなど、被害が拡大するおそれがあります。ですが、Cybereasonで侵入が検知できれば、端末を隔離するなどして被害を最小限に食い止められます。
実は、Cybereasonを導入後に今のところ一度も侵入されていないようですので、サーバーへの攻撃などが検知されたことはないのですが、少なくとも「侵入されたり、マルウェアなどが活動していたりすることが明確にわかる」ことには、とても安心感があります。

――サイバーリーズン・ジャパン株式会社が提供するSOCの印象はいかがでしたか?

繁倉氏：大いに満足しています。導入直後はどうしても誤検知が多少発生してしまうものですが、その際もすぐにミーティングを開いて対処いただきました。問い合わせに対する回答のレスポンスも早く、ユーザーの声を聞いて日々サービスを改善されていらっしゃることに好印象を持っています。

自社のエンジニアリソースをコア業務に集中

――そのほかに、Cybereasonを導入して良かったことはありますか?
繁倉氏：自社でセキュリティ対策要員を増やすことなく、セキュリティ対策のレベルを向上できたことです。もし、Cybereasonがなければ、弊社のエンジニアが侵入後の検知や対策を担当する必要があります。Cybereasonのおかげでエンジニアのリソースをコア業務に集中させられるので、会社にとっても大きなメリットが得られました。
また、運用の負荷が低いことも良かった点です。Cybereasonを導入しているのは、弊社が全国に持つ4つのセンターに設置してある、コンタクトセンター業務用のマシン約1,300台です。それらのマシンを普段から扱っているのは、コンタクトセンター業務に従事するオペレーターですから、何かインシデントが発生した際にも、最初に対応するのはオペレーターになります。
そうなると、オペレーターの業務負荷を増やしかねないのですが、CybereasonはSOCサービスが充実しているので、ほとんど負荷を増やさずに済みました。常にセキュリティのプロが後ろについてくれているような感覚を持てるのは、現場のオペレーターとしても心強いですし、セキュリティのことを特段意識せず業務に集中できるのはメリットだと思います。

―― EDRを使って今後どのようにセキュリティ向上をしていきたいか教えてください。

前田氏：変化し続ける外部環境に合わせて、私たちも歩みを止めず進歩していかなければなりません。さらなるセキュリティの向上を目指して、最も効果が見込めコスト面でもリーズナブルな打ち手を常に考えています。将来的には弊社で導入しているEDRのCybereasonで提供されているオプションサービスの導入も、有力な次の1手の一つとして検討しています。

優先順位をつけて対策を進めるべき

――最後に、EDRの導入を検討されている企業へメッセージをお願いします。

前田氏：サイバーセキュリティに終わりは存在しません。現状に満足せず、必要な対策を講じるべきです。しかし、すべてのセキュリティ対策を導入すればいいわけではありません。それでは、単なるリソースの無駄遣いになることもあります。
ですから、自社にとってのセキュリティ対策は何を一番に守るべきか優先順位を考えて、本当に必要かつ効果的な対策を見極めながらソリューションの導入を進め続けることが大切です。
中でも、CybereasonはGUIがすばらしく、検知力にも優れたEDRソリューションです。ヒューマンリソースもさほどかからないので、運用コストもかなり抑えられます。良いシステムだと思いますので、おすすめできます。

記載内容は取材時現在の情報です。

製品および記載内容に関するお問い合わせ

SCSK株式会社
https://www.scsk.jp/

ITインフラ・ソフトウェア事業本部 セキュリティソフトウェア部

〒135-8110 東京都江東区豊洲3-2-20 豊洲フロント
E-mail：cybereason-sales@scsk.jp
https://www.scsk.jp/product/common/cybereason/

Cybereason情報はこちら