事後対策に必須の「EDR」だけど、人手も予算も足りていない…あなたの会社ならどうする？

ますますサイバー攻撃が高度化・複雑化する昨今では、脅威の侵入を前提とした事後対策が欠かせなくなっています。そこで事後対策を効果的に行うためのEDR（Endpoint Detection and Response）が脚光を浴びていますが、導入を考えると「予算の確保」「効果測定の難しさ」「導入作業」「人手不足」などが課題となる企業も多いのではないでしょうか。本稿では、そんな悩みを抱えたある企業のケースを一緒にみてみましょう。

Z社について　従業員約1,000人の国内企業。年々順調に売上を伸ばしており、業界では風雲児的存在。

登場人物

Aさん：Z社の情報システム課セキュリティ担当主任。といってもほかの担当者は2人だけ。

B課長：Z社の情報システム課長。新しい技術にも積極的に興味を示すタイプで、最近は詳しくないながらも情報セキュリティが気になっている。

C氏：企業向けのセキュリティ対策を得意分野とする専門家。セキュリティ製品への的確な評価で知られ、ユーザー企業の間では信頼があつい。

うちの会社にもEDRを！だけど問題があった……

B課長、ちょっといいですか。

おや、どうした？ またテレワーク社員のVPN接続がうまくいかないとかかい？

いえ、今日は違うのでご安心を……。この記事※にあるEDRというセキュリティ製品なんですけど、うちも毎年の売上アップで成長してますし、この企業規模になってきたら絶対に必要だと思うんですよ。

お、新しい言葉が出てきたね。どうしてそれがウチに必要だと思ったの？

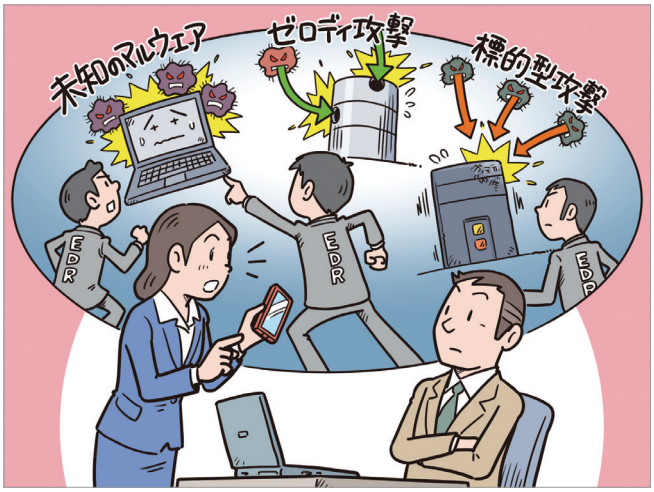
最新のセキュリティ脅威として最上位にあげられている未知のマルウェアやゼロデイ攻撃、標的型攻撃というのは、たとえ対策をしていても日々新たな攻撃を仕かけてくるために防ぎようがなく、知らない間に侵入してしまうため、もはや完全に防ぐことは難しいとされていますよね。

ゼロデイ攻撃や標的型攻撃とかいうのが危ないというのはこの前、君に教えてもらったね。それがどうしたの？

防ぎ切れないということは、いざサイバー攻撃によって侵入されてしまった場合はいち早く検知して、最適な対策を打つ「事後対策」というのが有効になるんです。この対策は現在セキュリティ業界で主流になりつつあるんですが、EDRがあればその事後対策が効果的に行えるんですよ。

なるほど、対策の仕方も変化しているんだね。有効なセキュリティ製品があるのなら、次の会議でぜひ提案してよ。

いえ、そこでなんですが……問題はEDRというのが、アンチウイルスなんかのセキュリティ製品と違い、入れてしまえばあとは製品にお任せ、というわけにはいかないらしいんですよ……。侵入を検知して対策をしようとしたときに、



最終的には人の判断が求められるみたいなんですね。

Aさんならできるんじゃないの？

とんでもないですよ！ わたし程度のセキュリティ知識の人間がゴロゴロいるような大企業でも、EDRを使っていないところが半分もあるらしいのに、事後対策までなんてとても手に負えませんよ。それにウチのセキュリティ担当者って、たった3人ですよ？ ただでさえ手がいっぱいなのに、さらに仕事を増やすのなら前からいっているようにですね、増員を……。

わかったわかった！ でも当社は安全・安心をお客様への売りにしているんだから、情報セキュリティだって大企業以上のことをやってやるぐらいの意識を持とうとお互いに話しているじゃないか。やはり事後対策ってのは、やらねばいけないようだし……何かうまい方法はないのかね？

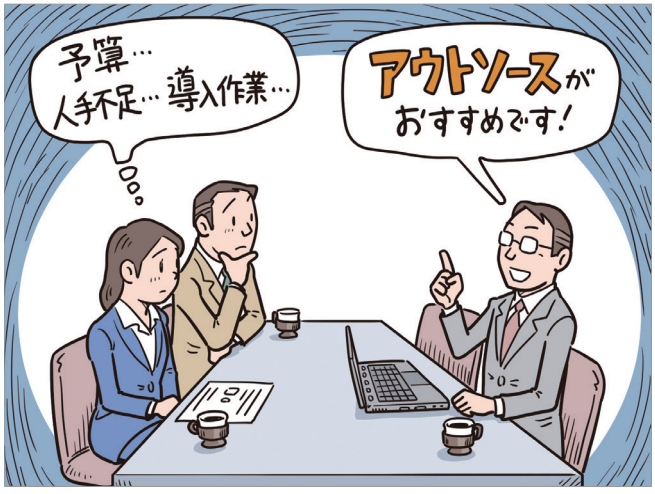
うーん、そうですね……。では一度、セキュリティ専門家のC氏に相談してみましょうか！

EDRの運用やコストが課題になっている企業は多い

それで……今回お越しいただいたのは、EDRを導入したいけど、セキュリティ担当者のリソースもスキルもとても足りないというご相談でしたよね。それならEDRの運用管理をアウトソースすればいいんじゃないですか？

アウトソース!? そんなサービスがあるんですね。

あるも何も、むしろEDR製品は運用管理サービスもセットというのが一般的なぐらいですよ。



そうだったんですか！ 外部の人たちに任せてしまえるのならば余裕ですよ、B課長！

い、いやちょっと待ってください？ そりゃ、セキュリティに限らずITの世界ではアウトソースはよくある解決策ですが、その、なんというかコストもまたかなりお高いというのが一般的じゃないですか。当社のIT予算はいまでもギリギリなので、そこまでの余裕はとてもとても……。

まあ、多くの企業がZ社さんと同じ状況だと思いますよ。実際、EDRの必要性はわかっていても、予算の確保や導入効果の測定が困難だったり、そもそも導入作業自体が負担になっていたり、さまざまな課題が導入を阻害している話はよく聞きますし。……それなら、この「EDR運用監視サービス」はどうでしょう？ ちょうど最近はじまったばかりのサービスです――。

圧倒的なコスパのEDR運用監視サービスがあった！

EDR運用監視サービス？ そのまんまの名前ですね。

確かにサービス名はそのものズバリですが、その内容はほかの同じようなサービスとは一線を画していて、Z社さんにもうってつけだと思いますよ。

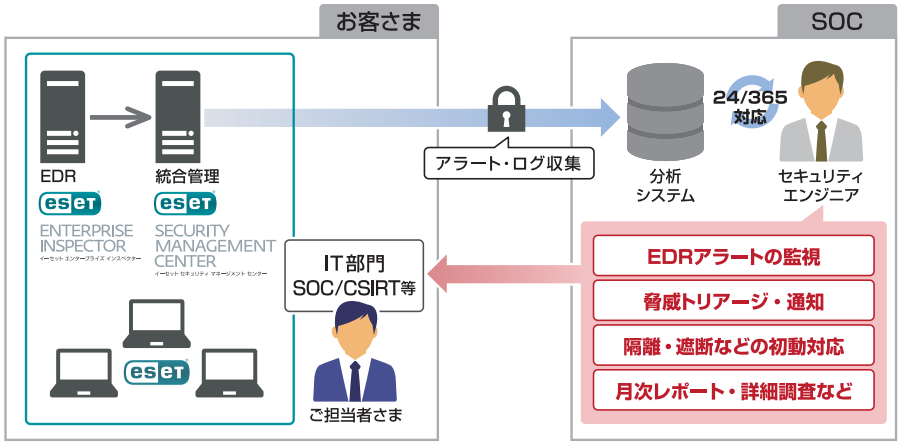
それはどんなサービスなんですか？

「ESET Enterprise Inspector（EEI）」というEDR製品はご存じですか？ 今回紹介するのは、このEEIを用いたEDR運用監視サービスなんです。このEDR運用監視サービスでは、専門のセキュリティエンジニアが24時間365日体制でEEIのアラートを監視・分析してくれます。何かインシデントが生じれば、その危険度に応じて速やかに通知し、侵害端末のネットワーク隔離や不正プロセスの強制停止など、インシデントレスポンスの初動対応まで行ってくれますよ。

それなら何かあっても、セキュリティ侵害を最小限に抑えられそうですね。特に24時間365日お任せできるのは嬉しいです！

このEEIは、 同じESET社のアンチウイルス製品「ESET Endpoint Protectionシリーズ（EEP）」とも連携するので、エンドポイント内にひそむ脅威を包括的に防御・可視化できるのも魅力です。

EDR運用監視サービス概要



- お客さま先に設置したESET Enterprise Inspector(EEI)を、SOCより24時間365日体制監視
- アラートが発生した際は多角的な分析を行い、危険度に応じてお客さまへ通知

※サービスプランによって提供内容が異なります

EDR運用監視サービス概要

確かに、セキュリティ製品ごとに運用方法が違うと負担になりますが、包括的に管理できるのは助かりますね。ただ、やはり気になるのが……。

コストですよね。このサービスは、運用監視対象端末1台あたり年額2,300円という圧倒的なコストパフォーマンスも特長なんです。

月額だと200円切りますね!

計算が早いですね(笑)。そう、高度セキュリティエンジニアの確保や、24時間365日体制の維持にかかるコストがハードルとなってEDRの導入に踏み切れなかった企業も、これなら手軽に事後対策を強化できるとうわけです。アラートの通知をメインとする「エントリープラン」と、端末隔離などの被害抑制まですべて行ってくれる「スタンダードプラン」の2つが用意されているので、企業のニーズに応じて選択することもできますしね。

B課長、わが社にはスタンダードプランがよさそうですね。これこそ当社が求めていたサービスじゃないですか!

うむ、これはもうすぐにでも話を聞いたほうがよさそうだな。

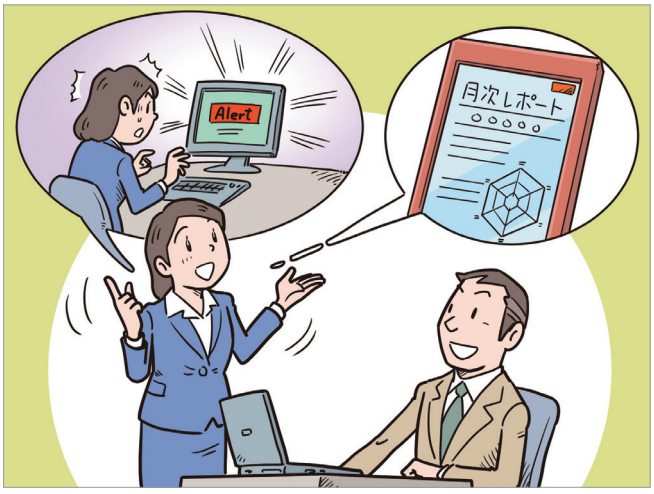
であれば、国内におけるESET社のセキュリティ製品の提供を引き受けているキヤノンマーケティングジャパンに連絡してみては?

はい、迅速に最適な対応こそセキュリティの基本ですからね!

数か月後のZ社に起こった変化とは……

B課長、ご報告です! EEIとEDR運用監視サービスのおかげで、うちの会社の端末に異常がないか、状態を把握できるようになりました! いまのところ感染などのトラブルもなく、健全な状態であることが確認できるので安心です!

それはよかった! 君たちセキュリティ担当の業務への負担も少ないみたいだね。



監視は24時間365日体制でやってくれますし、何かあったときには専門家が考えた対策方法と一緒に通知が来るので、あわてて相談する必要もありません。しかも月次レポートまで作成してくれるので、自分の仕事に専念できます!

それはよかった! さっそくだけどAさん、ほかの仕事も頼んでもいいかな?

B課長、すみません! ちょうど月次レポートが来たので確認しますね、それでは!

セキュリティ対策だけでなく、逃げ足も迅速だな……。

※「https://news.mynavi.jp/kikaku/edr_eei-1/」

EDR運用監視サービス

製品の詳細情報はこちら

▶https://eset-info.canon-its.jp/business/eei/mdr.html

ESET Enterprise Inspectorを用いたEDR運用監視サービスです。24時間365日体制で専門のセキュリティエンジニアがESET Enterprise Inspectorのアラートを監視・分析。危険度に応じて速やかにお客さまへ通知します。侵害端末のネットワーク隔離や不正プロセスの強制停止など、インシデントレスポンスの初動対応も行い、セキュリティ侵害を抑制します。

EDR (Endpoint Detection and Response)

eset ENTERPRISE INSPECTOR
イーセット エンタープライズ インスペクター

製品の詳細情報はこちら

▶https://eset-info.canon-its.jp/business/eei/

ESET Enterprise Inspectorは、エンドポイントレベルでのマルウェア対策を30年にわたり手がけてきたESET社の経験を基に開発されたEDR製品です。組織内の端末から収集したさまざまなアクティビティをもとに、端末上の疑わしい動きを検出・分析・調査し、組織内に潜む脅威をいち早く割り出し、封じ込めることができます。

ESET、ESET Endpoint Protection、ESET Enterprise Inspector、ESET Security Management Centerは、ESET, spol. s r.o.の商標です。
仕様は予告なく変更する場合があります。

製品に関する情報はこちらでご確認いただけます。

Home Page セキュリティソリューション ホームページ
canon.jp/it-sec

●お求めは信用のある当社で

開発元：ESET, spol. s r.o.

Canon キヤノンマーケティングジャパン株式会社
〒108-8011 東京都港区港南2-16-6 CANON S TOWER

2020年6月現在
MEDRU20061000MUR-649