エンドポイントセキュリティ事例 > EDR導入・運用

5年間の運用で培ったノウハウともたらされたメリット 次世代エンドポイントセキュリティ「EDR」運用の勘所とは？

働き方改革の推進やコロナ禍における感染拡大防止を背景としたリモートワークの普及に伴い、エンドポイントのセキュリティを強化するために「EDR（Endpoint Detection and Response）」の導入が加速している。マルウェア感染等のセキュリティインシデント発生の原因を追究し、適切な対策を施すツールとして脚光を浴びるEDRだが、導入の裾野が広がる一方、エンドポイントから収集される膨大なログへの対処をはじめ、運用に対する不安から導入に二の足を踏んでいる企業も少なくない。そこで、サイバーリーズン社の「Cybereason EDR」導入後、5年の運用実績を持つSCSKにEDR運用の勘所ともたらされているメリットを聞いた。

社内の端末約28,000台を Cybereason EDRで防御

コンサルティングから、システム開発、インフラ構築、そしてアウトソーシングに至るまで、ITに関するサービスをトータルで提供するSCSK。同社は2018年、社内のエンドポイントセキュリティの強化に向け「Cybereason EDR」を全社導入した。Cybereason EDRは、クラウド型のセキュリティソリューションで、エンドポイントのログを収集し、侵入したマルウェアやランサムウェアなどサイバー攻撃の兆候をクラウド上の機械学習エンジンによってリアルタイムに検知、対応を可能とするもの。Cybereason EDR導入の背景について、ITインフラ企画部 セキュアインフラ課の桂孝次は、こう説明する。

「コロナ禍以前の2017年からSCSKでは、働き方改革の一環としてリモートワークを推進していました。しかし、社外でのPC利用が増加する一方、従来のアンチウイルスや多層防御だけでは高度化するサイバー攻撃のリスクに対処しきれず、重要な情報資産を確実に守ることが困難であると危惧していたのです。加えて、万が一のマルウェア感染時にも、いち早く感染源や原因を突きとめ、対処可能な体制の構築も求められていました。これらの課題解決に向けて導入したのが、EDRだったのです」

数あるEDR製品の中でCybereason EDRを選択した理由は、社内で検証を行った結果、「未知の脅威を検知する能力が高いこと」「脅威への素早い初動対応とフォレンジック能力」「IT環境への負荷・既存環境への干渉の少なさ」「導入展開と運用のしやすさ」を評価したことにあった。

以来、5年にわたってCybereason EDRを活用し続けてきたSCSKであるが、現在ではコロナ禍によるリモートワークのさらなる拡大に伴い、防御対象となるPC、端末の数も導入当初の約19,000台から約28,000台まで増加しているという。「社外のネットワークからでもエンドポイントにおける怪しい振る舞いや、どのようなプログラムが実行されたか等、すべて検知・監視可能となっており、在宅勤務者のセキュリティ監視に非常に役立っています」と、桂は評価する。

サイバーリーズン社の 監視サービスも有効活用

SCSKはCybereason EDRの運用にどのように取り組み、最適化してきたのか。はじめに社内体制から見ていこう。マルウェア感染等の疑わしい挙動が検知された場合、一次報告として、24時間365日体制でセキュリティ監視を行うサイバーリーズン社の「Cybereason MDR（Managed Detection and Response）サービス」からアラートが寄

（左から）SCSK株式会社
ソリューション事業グループ
クラウドサービス事業本部
セキュリティサービス部
サイバーディフェンス課
セキュリティアナリスト
亀田勇歩

情報システム本部
ITインフラ企画部
セキュアインフラ課
後藤智成
桂孝次

せられる。そのアラートを受け付け、二次分析を行うのがSCSK社内のSOCチームだ。同チームでの分析結果がSOCポータル（インシデント情報共有基盤）にて共有され、ITインフラ企画部 セキュアインフラ課からインシデントの発生元と思われる社員への連絡やヒアリングが行われるというフローが構築されている。

社内SOCチームのリーダーとしてCybereason EDRの分析を担当する、セキュリティサービス部 サイバーディフェンス課 セキュリティアナリストの亀田勇歩は、インシデントレスポンスの一例を次のように説明する。

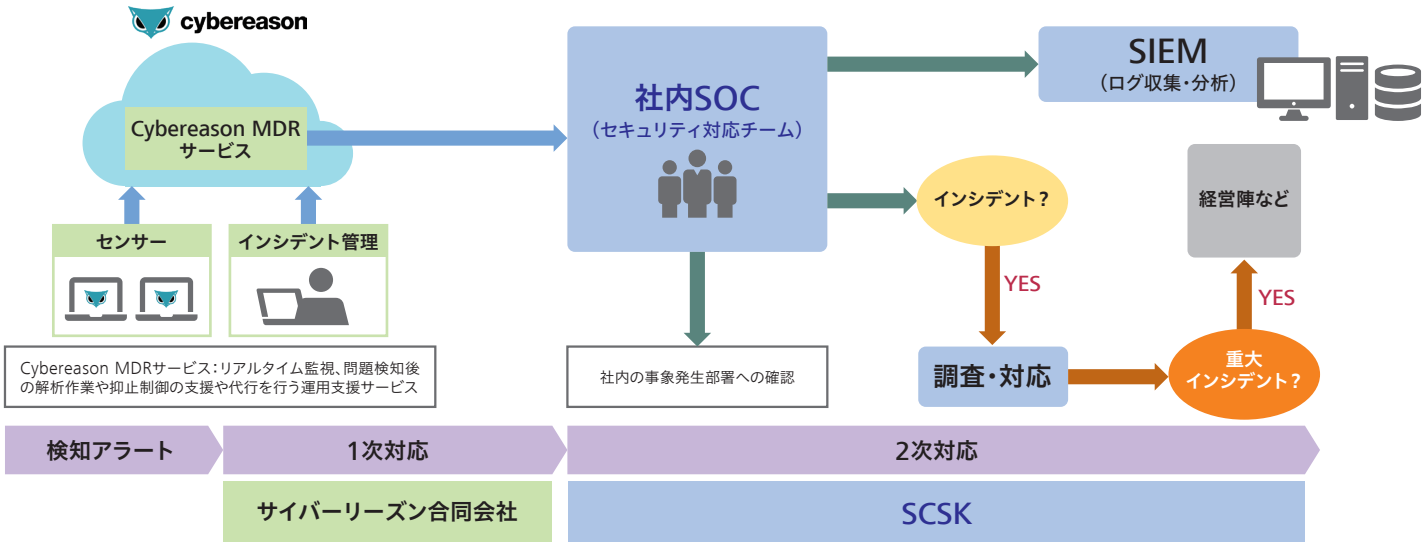
「一度、不審な動きをCybereason EDRが検知し、Cybereason MDRサービスからSOCチームにアラートが上げられたことがありました。すぐに調査を開始したところ、他のPCには影響が広がっていないことが判明。引き続き、事象を1つ1つ探りながら分析を重ね、最終的に社内の検証用アプリが原因であることが分りました。そうした分析を経たうえで、桂のチームに該当者へのヒアリングを依頼しました、このようにCybereason EDRの導入とMDRサービスの活用により、スピード感をもって事実関係を把握し、適切な対処が短時間で行えるようになっています」

社員に負担をかけず PCのセキュリティ強化が 可能な点も評価ポイント

続いて、Cybereason EDRの社員への展開をどのように行っているのか、見ていこう。SCSKでは、新規PCを社員に配布する際には、Cybereason EDRのエージェントがインストールされた状態で提供しているという。ITインフラ企画部 セキュアインフラ課の後藤智成は、「基本的な設定もキッティング時に行っており、社員にはCybereason EDRの個別設定を行うための簡単な説明書をPCと一緒に梱包、配布しており、箱を開ければすぐに使えるような状態にしています」と説明する。

エージェントのアップデートについても、Cybereason側からの通達

図 SCSKにおける「Cybereason EDR」を活用したセキュリティ運用の体制図



をPC内のエージェントが受信すれば自動的に実施。「社員がアップデートに際して煩わしい作業を行う必要はありません。そもそも、社員のPC画面にはCybereasonのコンソールやポップアップさえも表示されないので、稼働もアップデートも全く意識することなく行われています。導入してから5年間が経ちましたが、社員に対してアップデートの要請やアナウンスをしたことは一度もありません」（後藤）という。

このほか、運用側として、Cybereason EDRがクラウド型のセキュリティサービスであることも大きなメリットであるという。

「あらかじめエージェントをPCにインストールしておくだけで済み、別途、大がかりなシステム構築などの作業も発生しません。加えて、PCの利用場所が社内社外に関わらず、同様のセキュリティ機能が提供されている点も、クラウドサービスとしてのメリットとして捉えています」（後藤）

継続的な機能強化により運用負荷も軽減

Cybereason EDRを活用し続ける中で、この5年間で実施された様々な機能強化による恩恵も授かっているという。

「Cybereason EDRは毎年のようにバージョンアップしていますが、運用側の視点からは管理画面がどんどん使いやすくなっていることが大きな評価ポイントです。当初は文字情報が中心だったセキュリティインシデントに関する情報、およびPCの詳細な情報などが、現在ではビジュアル的に分かりやすく表示されるようになり、状況が一目で把握できるようになっています」（桂）

亀田も「同様に、この感染はどのプロセスに紐づいていており、誰が何時、どのようなファイルを開いて感染したのか、管理画面上からツリー型構造で可視化されています。以前は専門的なスキルを持った担当者でなければ読み解けなかったものが、直感的に理解できるよう更新されており、より効率的な分析が行えるようになっています」と評価する。

Cybereason MDRサービスも強化されており、検知時のアラートが以前よりもさらに早くなったことに加え、AIを活用した解析により、誤検知も減っているという。

「私たちのようなインシデント分析チームにとっては、一次報告の誤検知が少なく、かつ、アラートが早ければ早いほどセキュリティ対応の初動に素早くとりかかれるので、とても助かっています」（亀田）

Cybereason EDRの継続的な運用によって、社員が利用するPCのセキュリティを確実に維持し続けるSCSK。事実、Cybereason EDRによる常時監視が行われていることが社員のセキュリティ意識をさらに向上させるといった効果ももたらし、リモートワークが拡大した状況にあっても、セキュリティインシデントと思しき事象の発生は数か月に数件程度に留まっているという。

このように大きな効果をもたらしているCybereason EDRだが、セキュリティに関する専門知識を有する社員や、セキュリティ専任の担当者を有していない企業は少なくなく、EDRの導入に踏み出せないといった悩みを抱えている情報システム担当者は多いと思われる。これに対して桂は、EDR導入を検討している企業の担当者について、次のようにアドバイスを寄せた。

「Cybereason EDRには、Cybereason MDRサービスといった監視サービスも提供されており、アラートを発するだけでなく、対処が必要と思われる事象についてアドバイスも与えてくれます。そうしたサポートサービスを活用することで、EDRの活用、ひいてはセキュリティ強化に向けた運用のノウハウを蓄積していくことが可能となります」（桂）

そして、自社運用で培った知見やノウハウを基に、SCSKはCybereason EDRの最適な運用を見据えた導入提案、および設計や構築サポートを可能としている。EDRの導入を検討しているのであれば、ぜひ一度、SCSKに相談してみてはいかがだろうか。

製品および記載内容に関するお問い合わせ

SCSK株式会社

ITインフラ・ソフトウェア事業本部 エンタープライズ営業部
〒135-8110 東京都江東区豊洲3-2-20 豊洲フロント
Email：cybereason-sales@scsk.jp

お問合せフォーム

製品ご紹介