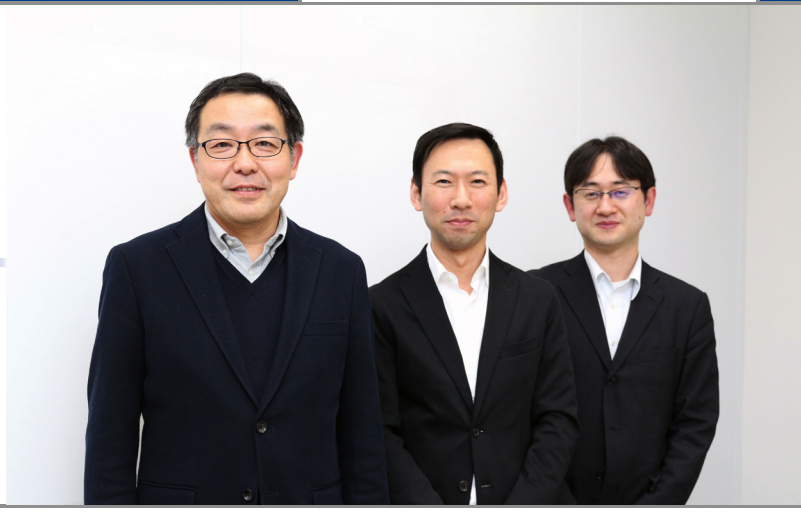
導入事例 Case Study

SoftBank
http://tm.softbank.jp/

ソフトバンク株式会社



ソフトバンク社内 6 万台の PC に「Cybereason」を導入、標的型攻撃に対するセキュリティを強化

ソフトバンクでは端末に侵入したマルウェアを迅速に検知し、機密情報が漏えいを防ぐセキュリティ対策として社員とコールセンターの PC に「Cybereason」を導入しました。近年、さらに巧妙化しているサイバー攻撃に対しては、マルウェアの侵入を防ぐ水際対策だけでは十分ではなく、侵入したマルウェアを迅速に検知し機密情報が漏えいする前に対策を施すエンドポイントセキュリティ対策が重要です。「Cybereason」により従来は平均 30 分程度要していた侵入検知が、リアルタイムに行え未知のマルウェアも検知できるようになり、より強固なセキュリティを実現しました。

課題と導入の効果

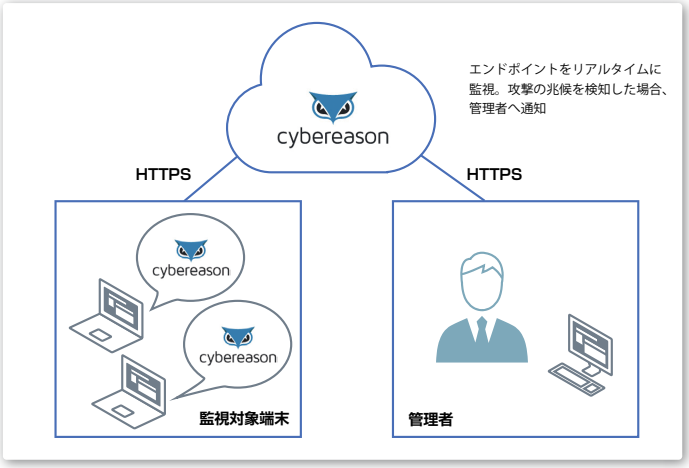
課題 従来の不正侵入検知対策では大量のログを解析する必要があり管理者に負荷がかかっていました。

▶ **効果** 「Cybereason」はログ収集と解析を自動化して脅威情報をリアルタイムで提供するため管理者の負荷は減少しました。

課題 不正侵入検知型製品は端末やサーバに負荷がかかるものが多くエンドユーザの業務に支障をきたします。

▶ **効果** 「Cybereason」は端末の負荷が少ないため、エンドユーザへの影響はほとんどありませんでした。

最近のサイバー攻撃は高度化、組織化しており、資金を提供する者、マルウェアを作る者、プラットフォームを提供する者、攻撃を実行する者などが複数の国に分かれて活動しているのが実態で、攻撃者は特定の企業を標的に定めると、攻撃が成功するまで執ようにアタックします。こうした攻撃を企業が完全に防御するのは容易ではありません。そこで重要になるのはマルウェアの侵入を許してしまう事態をあらかじめ想定し、可能な限り早急に侵入を検知したのち、被害を最小限に食い止める対策を講ずることです。



ソフトバンクでは 2014 年に「SoftBank Security Operation Center」という組織を立ち上げて 24 時間 365 日専門スタッフによる社内システムの監視を実施しています。2015 年には脅威が増大しつつあった標的型攻撃に備えた侵入検知型ソリューションの導入に向け複数の製品を評価した結果、「Cybereason」を選択しました。導入対象は社員が利用する PC およびコールセンターで利用する PC の約 6 万台です。

従来のセキュリティ体制でも社内ネットワークに接続した PC の疑わしい挙動を検知することは可能でしたが、挙動開始から検知までに平均 30 分はかかっていました。また、マルウェア感染を疑われる PC を特定してネットワークから切り離し、デジタル・フォレンジックを完了するのに平均 3 週間を要していましたが、「Cybereason」を使えば検知はリアルタイムに、さらにデジタル・フォレンジックは即日完了します。大幅な時間短縮によって、機密情報が外部に送信される前に対処することが可能になりました。

ユーザの声

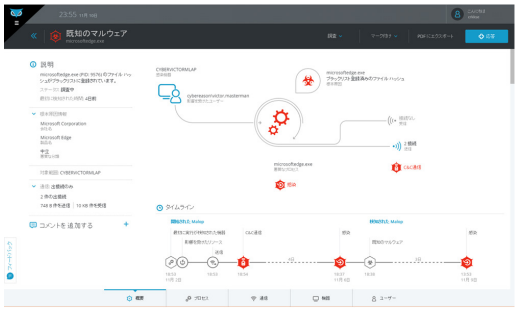
ソフトバンク株式会社
セキュリティ事業本部
本部長
清水 啓一朗 氏

「Cybereason」はサイバー攻撃を実行する側の手口を熟知したエンジニアが開発しているのが特長で、攻撃者の用いるツールや外部との不正な通信、感染を拡大させる手段といった攻撃パターンについて、端末から取得したログをクラウド上のAIエンジンによって解析しています。従来のパターンマッチングを用いるマルウェア検知ソフトは未知のマルウェアや攻撃には対処できませんが、「Cybereason」はサイバー攻撃特有の活動を常時監視しているので、未知のマルウェアであっても不正な挙動をすれば即座に検知できる点が優れています。「Cybereason」は既存のセキュリティ対策では防げない脅威に対抗するための製品と位置づけているため、当社では従来のセキュリティ対策製品と併用して稼働させ、対策を強化しています。

ソフトバンク株式会社
セキュリティ事業本部
サポートデスク課 課長
粂川 智秀 氏

「Cybereason」を使った実際の運用では、例えば社員がマルウェアに感染した添付ファイルを開いてしまった場合、一定の潜伏期間の後に活動を開始するとリアルタイムにアラートメールが送信されます。セキュリティ担当者は「Cybereason」の管理コンソールから問題の端末を特定してネットワークから切り離し、危険なプロセスを削除するといった対応を即座に実施することで、機密情報を抜き取られる被害を未然に防げます。従来は大量のログを人力で解析していたので、脅威の検知から端末の特定、脅威の除去といった各プロセスにセキュリティの専門知識を持ったアナリストの力が必要でしたが、「Cybereason」はアナリスト業務を代行してくれるので、専門知識がない担当者でも運用管理が可能になりました。製品導入後のチューニングも必要ありません。

管理コンソールの「概要」画面では検知した既知 / 未知のマルウェアが見える化される



特定のマルウェアについてブレイクダウンすると、侵入された端末、実行されたプログラム、端末の通信先、攻撃などのタイムラインが、管理コンソール上にアイコンとして表示される

ソフトバンク株式会社
セキュリティ事業本部
サービス企画課 課長
蝦名 英樹 氏

侵入検知型セキュリティ製品の選定に当たり「Cybereason」を検証しました。テスト環境でマルウェアをどのように検知するか調べた際に、一般のマルウェア検知型製品とは違って、サイバー攻撃特有の挙動を監視することで未知の脅威を検知できる点を評価しました。実運用で重要となる端末負荷については、他社製品では動作が遅延したり挙動が不安定になることも少なくありませんが、「Cybereason」は非常に負荷が小さく、エンドユーザがその存在に気付かないほどでした。ひと月ほどの検証期間を経て導入を決定したのち、一部の部署に先行導入したところ実運用で問題が発生しなかったので、その後 1 日数千台ずつ一気に 6 万台まで配布を実施しましたが、トラブルなく本格的な運用を開始できました。

導入企業情報

SoftBank

会 社 名：ソフトバンク株式会社
本　　社：東京都港区東新橋 1-9-1
設　　立：1986 年
U　R　L：http://www.softbank.jp/
従業員数：約 17,700 人

※パンフレット記載内容は、2017 年 1 月現在のものです。