DARKTRACE

ケース スタディ

ソニーライフ・エイゴン生命保険株式会社 様

AEGON Sony Life

概要

業界

- 保険

課題

- 保険業として顧客情報の保護は最重要課題
- 企業の相次ぐ情報漏えい事故を背景に、サイバー攻撃や内部不正などの脅威を軽減するための対策が急務
- 社内の限られた社内リソースでのセキュリティ運用

結果

- ログを見ても把握できなかった社員の行動を可視化でき、リアルタイムに異常を検知
- 異常検知後の分析・調査の運用負荷を軽減し、生産性が大きく向上
- 万が一、情報が流出するようなインシデントが発生した場合でも、その後の対処を迅速に進められる

ビジネスの背景

ソニー生命保険株式会社と年金保険のリーディングカンパニーである蘭エイゴン・インターナショナル B.V.との合弁によって設立されたソニーライフ・エイゴン生命保険株式会社（以下ソニーライフ・エイゴン生命）は、「個人年金を人生年金へ」というスローガンを掲げて年金保険を中心としたビジネスを展開し、最新のデジタルテクノロジーを活用してビジネスを変革する「デジタル戦略」を推進しています。

> SIEM 製品では、どこから何のログを取るか設定し、ログを確認するための管理画面を作り込まなければなりません。その点、Darktrace は導入も運用管理も容易でした。
>
> **ソニーライフ・エイゴン生命 情報システム部 システム業務課 統括課長 馬場 正晴 様**

課題

一般の事業会社よりも、機微な個人情報を預かっている生命保険会社にとって、顧客情報の保護は極めて重要な課題です。ソニーライフ・エイゴン生命でもデジタル戦略を推進する以前から、さまざまなセキュリティ対策を講じてきましたが、情報漏えい対策をいくら強化しても内部の不正行為を完全に防ぐことは難しく、また標的型攻撃などのサイバー攻撃によって社内ネットワークに侵入されれば、アカウントを乗っ取られて重要なデータが盗まれる恐れもありました。そこで同社では、デジタル戦略の展開をきっかけに、こうした脅威をさらに軽減するための対策を導入することを決断し、2015 年にセキュリティ対策を強化するロードマップを描き、2016 年に実施する計画を立案、その一環として内部ネットワークのモニタリング強化を掲げました。

同社の情報システム部には30 名程度が所属していますが、セキュリティ対策を専門とするメンバーは多くはなく、セキュリティ対策の検討にあたっては、モニタリングが継続できるかどうか、また、限られたリソースに対していかに運用を省力化できるかも課題でした。SIEM ではログの収集は自動化できますが、"不正の可能性がある"と判定するルールは人間が決めなければなりません。厳しいルールにすればアラートの数が膨大になり、緩やかなルールでは不正を見逃す恐れもあります。さらに、新たな手口のサイバー攻撃が登場した場合にルールを変更する必要があり、運用は容易ではありません。

（※）Enterprise Immune System の導入・運用は京セラコミュニケーションシステム株式会社が行っています。

解決策

さまざまなセキュリティ対策を検討する中で、同社はネットワークを流れる通信パケットを監視して不正を検知するツールがあることを知り、複数ツールの中から最終的に選定したのが、Darktrace が提供するEnterprise Immune System でした。2016 年夏からのPoV（※）を経て、同年 12 月から本格稼働を開始しました。

Enterprise Immune Syste mの大きな特長は、不正を検知する機能に AI 技術の一種である機械学習を活用していることです。ネットワーク内の通信パケットを分析し、正常な状態（不正が発生していない状態）の通信パターンを自己学習します。学習後は流れるパケットをリアルタイムに監視し、正常な状態のパターンから外れた際に「異常が発生した」と判断し、アラートを発する仕組みです。例えば、大容量データの複製や移動、外部の情報機器との通信、普段使っていないプロトコルの利用、労働時間帯以外における活発な行動、通常はほとんど利用しない Web サイトからの実行可能ファイルのダウンロードなどを検知しますが、業務上で頻繁に大容量データを複製するユーザーの行動に対しては「異常が発生した」とは判断しません。

また、Enterprise Immune System はアプライアンス製品として提供されており、社内ネットワークのスイッチに接続し、簡単な設定を行えば、後は自動的に学習を開始します。ソニーライフ・エイゴン生命では、Enterprise Immune System をデータセンターのコアスイッチに接続し、内部ネットワークを流れるすべてのパケットを収集しています。

> 機械学習によって正常な状態を学習し、そうでない場合は危険度によってアラートを上げてくれます。不正を判断するルールを人間が設定・変更する必要はありませんので、運用の省力化という要件にマッチしました。
>
> **ソニーライフ・エイゴン生命**
> **情報システム部 IT セキュリティマネージャ**
> **磯貝 徹 様**

利点

Enterprise Immune System の導入により、ログを見ても把握できなかった社員の行動が可視化でき、リアルタイムに異常を検知できるようになりました。現在のアラート発生件数は、平均すると 1 日に 1 件程度で、ほとんどが業務上の要件によって、通常とは異なる行動を取ったために発生したアラートです。PoV の期間も含めて、今まで外部からのサイバー攻撃や内部の不正による被害は発生していませんが、万が一、情報が流出するインシデントが発生した場合でも、その後の対処を迅速に進められます。

（※）Proof of Value：4 週間の導入前検証。.

お問い合わせ

Tokyo: +81 3 5456 5537
North America: +1 415 229 9100
Europe: +44 (0) 1223 394 100

japan@darktrace.com
darktrace.jp