DARKTRACE

ケース スタディ

山口朝日放送株式会社 様

概要

業界

- メディア

課題

- 急速に進む放送機器のIoT化
- 放送に支障をきたす恐れがないセキュリティ対策の必要性

結果

- 日本国内の放送局で初めてEnterprise Immune Systemを導入
- ルールベースの製品をすり抜ける未知の脅威をリアルタイムに検知
- テープレス化・フルIP化が進むテレビ局の放送システムの安定稼働に貢献

ビジネスの背景

山口朝日放送株式会社（以下yab）は、山口県を主な放送対象地域とするテレビ朝日系列のテレビ局で、キー局が制作する番組のほか、自社制作の報道番組や地元に密着した情報番組を毎日放映しています。2018年10月に開局25周年を迎えるyabは、変化の速いメディア業界にあって、地域に根差した放送局としての足場をさらに固めて行きながら、柔らかな発想を大切にし、新しいチャレンジを続けています。

課題

放送業界では、長年にわたりテープを用いた撮影・編集が主流を占めており、テープに記録されたものを物理的に受け渡しする慣習が続いていました。最近はファイルベースのシステムに移行しつつあり、取材カメラで撮影する映像をデータファイルとして保存して、PCで編集、サーバーから送出するようになってきています。

yabも2016年から全社的に映像素材のファイル化を進めており、放送機器をITネットワークに接続したり、映像データを社内イントラ上で取り扱うことが格段に増える中、ITセキュリティ対策の強化は急務でした。

一方で、放送局に特化した専用のアプリケーションソフトを使用しているため、放送機器メーカーで動作検証がとれていないOSのアップデートやエンドポイントセキュリティのソフトウェアを放送系のシステムにインストールすることは基本的に難しい現状があります。

また、一刻を争う報道の現場では、情報収集目的で様々なウェブサイトに素早くアクセスする必要があります。視聴者など社外の不特定多数の人々から様々な媒体を通じてニュースの情報提供を受けることも多く、URLフィルタリング機能による閲覧制限、アプリケーションコントロールによるソフトウェアの実行停止などの対策は、円滑な取材業務に支障をきたすことも考えられます。

（※）Enterprise Immune Systemの導入・運用はNTTアドバンステクノロジ株式会社が行っています。

解決策

このような状況に最適なセキュリティ対策を追加するにあたり、yab はエージェントレスの製品を活用して、まずは内部ネットワークを流れるトラフィックを監視することが第一歩だと考えました。ネットワークレイヤで稼働するセキュリティ製品を複数検討する中で、Darktrace が提供する Enterprise Immune System に出会いました。振る舞い検知やパターンマッチングに基づくルールベースの製品をすり抜けてしまうサイバー攻撃、さらにサンドボックス製品を組み合わせても対処できない未知の脅威や内部脅威に対しては、内部ネットワークを流れる通信パケットを常に分析し、正常な状態の通信パターンを独自の AI で自己学習し続けることで異常をリアルタイムに検知し、アラートを発する Enterprise Immune System だけが確実に対処できると考え、POV (※) を開始しました。

Enterprise Immune System はアプライアンス製品として提供されており、yabでは社内ネットワークの L3 スイッチにミラーポートを設定してアプライアンスを接続し、内部ネットワークを流れるすべての通信パケットを収集・分析しています。分析の様子はウェブブラウザ上で稼働する Darktrace 独自の 3D 可視化ツールである Threat Visualizer で一元的かつリアルタイムに把握することができます。

POVを開始して間もなく、yabの社内ネットワークである端末が1時間毎に不審なビーコン通信を開始していることを Enterprise Immune System が検知・可視化しました。導入済みのファイアウォール製品がこの通信をブロックして実害はありませんでしたが、Darktrace がリアルタイムにこの異常な挙動を可視化できたことで、迅速にこのビーコンを発信していたアプリをアンインストールすることができました。ファイアウォールのログを頻繁に細かく分析する手間に照らすと、Threat Visualizer で視覚的かつリアルタイムに異常を把握できることは非常に有益です。

利点

yabでは情報漏えいや放送業務に支障をきたす恐れがある深刻な脅威や被害は今まで発生していませんが、昨今テレビ局における映像制作・放送業務で使用されるほとんどのデバイスが IP アドレスを持つようになり、かつては考えられなかったような勢いでネットワークに接続される中、他局に先駆けて日本国内の放送局で初めて Enterprise Immune System を導入できたことは、社内外に大きな安心感をもたらしました。放送局におけるテープレス化・フル IP 化が進む一方、放送機器毎にセキュリティアップデートを施すことが難しい業界特有の事情に鑑みて、Enterprise Immune System はテレビ局の業務と特に親和性が高い製品と言えます。

> 放送機器の IoT 化がますます進む一方、これらをサイバー攻撃から保護するためにセキュリティパッチを適用したりエンドポイントセキュリティ製品を導入することは、誤動作や誤検知等により放送業務を予期せず止めてしまう可能性に照らすと非常にハイリスクです。また、セキュリティを担保しながらも不自由なくデバイスを使いこなすことは即時性が求められる報道の現場に必要不可欠です。パケットキャプチャをするだけでネットワークの定常状態を自己学習し、未知の脅威を自動的に可視化・検知できる Darktrace は、多くの放送局が現在抱えている IT セキュリティ上の課題を解決できる最適な製品だと思います。

山口朝日放送株式会社 技術局
技術部 副部長 中嶋 健聖 様

(※) Proof of Value: 4 週間の導入前検証。

お問い合わせ

シンガポール: +65 6804 5010

日本: +81 (03) 5456 5537

ヨーロッパ: +44 (0) 1223 394 100

japan@darktrace.com
darktrace.jp