DARKTRACE

ケース スタディ

京阪ホールディングス株式会社 様

こころまち つくろう
KEIHAN

概要

業界

- 陸運業、その他

課題

- グループ各社のITネットワークにおける一元的かつ即時的なセキュリティアセスメント
- 一般的なサンドボックス製品やエンドポイント防御によるシグネチャベースの脅威検知の限界

結果

- 既存のSIEMや出入口対策に加えて内部ネットワークの完全可視化を実現
- メンテナンスフリーでAIが通信の異常度に応じて即座にアラート

ビジネスの背景

京阪ホールディングス株式会社（以下、京阪ホールディングス）は、約 50 社におよぶ企業で構成される京阪グループの持株会社で、運輸業、不動産業、流通業、レジャー・サービス業の 4 つのコア事業を営んでいます。京阪間と滋賀が地盤の鉄道事業を核に、幅広い事業フィールドで「快適な生活環境を創造」し、社会に貢献しています。

> SIEM製品の運用において、例えばファイアウォール設定が変更されるとSyslog形式も変わるため、SIEM製品のメンテナンスが必要不可欠ですが、機械学習の対象として通信パケットを収集するEnterprise Immune Systemは、境界の装置が何であれ、設定を変更することなくあらゆる脅威を即座に自動検知できます。
>
> **京阪ホールディングス株式会社 経営統括室 IT推進部 課長 馬場 康弘 様**

課題

様々な業種のグループ会社を統括する持株会社である京阪ホールディングスは、2018 年以降、各事業を行うグループ会社の IT ネットワークを統合し始めており、各社の情報セキュリティアセスメントを京阪ホールディングスから一括で実施したいというニーズがありました。また、京阪グループではクレジットカード事業やグループポイント運営事業も行っており、個人情報をより厳重に保護するためにも、従来から対策を行っている SIEM による通信ログの一元管理・分析、サンドボックス製品やエンドポイント防御によるルール・シグネチャベースの脅威対策に加えて、内部の不正行為やコンプライアンス違反による情報漏えいのリスク、また攻撃が顕在化する前に脅威の予兆や不正が疑われる通信の有無なども含めて漏れなく監視したいと考えていました。

内部ネットワークの挙動を監視する製品を複数のグループ会社で検証していましたが、いずれも脅威をパターンマッチングによって既知か未知かを判断したり、グループ会社に赴いた上で不審な通信や振る舞いを発生させた端末をサンドボックスに隔離して逐一ヒューリスティック調査を行ったり、加えて個々のシステムの膨大な通信ログを確認する必要もあり、人的リソースに限界を感じ始めていました。

あるグループ会社において、人手によるものとは思えないアクセスが数百回にわたりファイルサーバーに対して行われたことがあり、パターンやルールに基づく標的型攻撃対策製品を現地のサーバーにインストールしてみたものの、原因を突き止めることができませんでした。内部ネットワークに侵入した攻撃者により人間の能力を遥かに超える速さで実行されるラテラルムーブメント、悪意の有無に関わらず常に存在する内部脅威など、サイバー攻撃の予兆を素早く検知するためにも、リアルタイムかつ視覚的に内部ネットワークの通信を可視化でき、かつ遠隔で運用を自動化できる製品を導入したいと考えていました。

解決策

グループネットワークの統合を進める中で監視すべきデバイスの数は増え続けており、導入時の手間を最小限に抑えるという観点で、エージェント型やインライン型の製品ではなく、内部ネットワークのコアスイッチに接続するだけでインストールでき、1時間程度であらゆるデバイスの普段の通信パターンを機械学習し始める Darktrace の Enterprise Immune System で PoV（※）を実施することを決めました。

人間の免疫システムに着想を得て開発された Enterprise Immune Systemは、ネットワーク内の通信パケットをポートミラーリングによってアプライアンス内で収集・分析し、京阪ホールディングス固有のネットワークの生活パターンを自己学習し続けます。流れるパケットは Darktrace 独自の 3D 可視化ツールである Threat Visualizer によってウェブブラウザ上で一元的かつリアルタイムに監視でき、定常状態から外れた際に「異常が発生した」と判断し、アラートを上げる仕組みです。

SIEM 製品は導入に際して既存のシステム構成や、業務や組織の実態に合わせた精緻なチューニングが必要で、導入後もシステムの変更や、攻撃手法の変化、セキュリティポリシーの変化に合わせてその都度設定を変更する必要がありますが、Enterprise Immune System は異常を判断するルールをシステム管理者が設定・変更する必要がなく、AI が通信の異常度に応じてリアルタイムにアラートを発します。

京阪ホールディングスでは、情報漏えいや業務に支障をきたす恐れがある深刻な脅威は検知されていませんが、業務上やむを得ず通信プロトコルとして SMB1.0 クライアントを有効化した際に Enterprise Immune System がその変更を即座に検知するなど、SMB の脆弱性を突いたランサムウェアがかつて世界中で猛威を振るったことに照らすと、脅威を未然に防ぐという観点で大きな安心感に繋がりました。また、あるファイルサーバーからダウンロードされたデータ量と同じデータ量のファイルをアップロードしようとしていた通信、あるいはウェブブラウザのアドオンを追加した際に PC が一時的に発した不審な通信なども、Enterprise Immune System はリアルタイムに検知・可視化しました。

利点

グループ各社の IT ネットワークの統合を推進する中、Enterprise Immune Systemの導入前後で監視対象の端末数が増加しており、従来のツールでは決して把握することができなかった内部ネットワークのあらゆる通信をリアルタイムかつ網羅的に確認するという意味では一時的に運用負荷が増えた実感はあるものの、エージェント型製品とは異なり、通常業務に何ら影響なくパケットのヘッダー情報を自動的に収集し続けるだけであらゆる異常を検知できる Enterprise Immune System は、長期的には費用対効果に見合う製品だと確信しています。

また、Enterprise Immune System は子機を設置することで子機が収集したパケット情報を親機に集約することで別拠点にまたがるトラフィックも一元的に監視することができ、加えてオンプレミス環境のみならずクラウドオンリーのネットワーク環境にインストールすることも可能です。ネットワークの規模が今後大きくスケールしても、事前設計やチューニングに煩わされることなく AI が通信状態を自動学習し続けるため、少人数でも導入・運用しやすい製品です。

（※）Proof of Value：4 週間の導入前検証。

お問い合わせ
株式会社ピーエスアイ
TEL: 03-3357-9980
Email: support@psi.co.jp