DARKTRACE

ケース スタディ

福岡ひびき信用金庫 様

あなたと共感、ハーモニー・バンク
福岡ひびき信用金庫

概要

業界

- 金融

課題

- 本社のファイルサーバーと各支社のクライアント間の通信状況をリアルタイムに把握したい
- 先駆的で信頼できるITインフラの自社構築を推進しており、最先端のセキュリティ製品が常に必要

結果

- 内部ネットワークの生活パターンの機械学習が深まるにつれて少人数運用でも安心感が向上
- 脆弱性対策における軽微な対策漏れも即座に把握

ビジネスの背景

福岡ひびき信用金庫（以下、福岡ひびき）は、北九州市八幡東区に本店を置く、九州で最大級の規模を誇る信用金庫です。1924年に設立され、2001年に北九州八幡信用金庫と若松信用金庫が合併したことを機に現在の金庫名となり、福岡県一円、山口県下関市、大分県中津市を営業区域として地域密着型の金融サービスを提供し、約100年にわたって地元の経済を支えてきました。

> 各クライアントに個別にインストールした上で事前設定が必要な振る舞い検知などの製品に比べて、社内ネットワークのコアスイッチに接続してから1時間程度で自動的に学習を開始するEnterprise Immune Systemは、ITネットワークの複雑な知識がなくても、少人数であっても導入・運用が容易です。
>
> **福岡ひびき信用金庫 事務部 システムグループ グループ長 吉田 篤史 様**

課題

福岡ひびきは、システムの内製化を基本に、最近では業務系システムの仮想化を推進するなど、業界において他に先駆けた取り組みを行う信用金庫としても知られています。未知の脅威が猛威を振るう中、信頼性が高いITインフラを運用する金融機関として、サイバーセキュリティ製品は常に最先端のものを導入すべきであるという認識がありました。

また、ITインフラの大部分を社内のシステムグループが自社で構築・保守している関係上、システム管理者の負担を軽減しながら、限られた社内リソースで効果的なセキュリティ運用を実現したいと常に考えていました。さらに、ネットワークの仮想化を進める中でファイルサーバーを本社でまとめて運用している関係上、本支社合わせて3,000近くのデバイスから本社のサーバーに不審なパケットが入ってこないよう、各支社のクライアントとサーバー間の通信を包括的かつリアルタイムに可視化することで安心感を得たいという気持ちがありました。

解決策

福岡ひびきは、これまでにサンドボックスや統合脅威管理（UTM）、IPSなどの様々なセキュリティ製品を導入・活用してきましたが、これらの製品群でネットワークを逐一監視し続けるための人的リソースに限界を感じていました。福岡ひびきでは従来から最新のセキュリティ対策を導入し続けており、業務運営に支障をきたす恐れがある深刻なサイバー脅威や情報漏えいなどの被害は今まで発生していませんが、2017年にWannaCryをはじめとするランサムウェアが大流行したこともあり、SMBによる通信が急増する、あるいは普段アクセスがないPCから重要なサーバーに対する突然のアクセスやダウンロードが開始されるなどの異常な挙動やゼロデイの脆弱性、さらには内部脅威が発生するなど、万一の場合に備えて包括的かつ自動的に事前対処できるセキュリティ製品の導入が急務でした。このようなサイバー脅威の新時代にマッチする製品で、投資対効果に見合うものであれば積極的に検討するという企業風土や経営層の理解もあり、2018年7月にDarktraceのEnterprise Immune Systemに出会ってまもなく、POV（※）を開始しました。

人間の免疫システムに着想を得て開発されたEnterprise Immune Systemは、独自のAI技術を駆使することで、あらゆる種類のネットワーク環境においてサイバー脅威の自動検知・可視化から自動遮断まで包括的なセキュリティソリューションを提供しています。POVでは、アプライアンス製品であるEnterprise Immune Systemを福岡ひびきの内部ネットワークのL3スイッチに接続し、ポートミラーリングによってファイルサーバーに集まる全ての通信パケットを収集することで、福岡ひびき固有のネットワークの生活パターンを自動的に常時機械学習しながら、その様子を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直感的に監視しました。

ビジネスに危機をもたらす深刻な脅威やサイバー攻撃を発見するという事態は免れているものの、POVを開始した直後に、かつて導入してアンインストールしたはずのセキュリティ製品が診断用のポートスキャンを続けていたことや、SMBのレガシーバージョンが未だ有効な端末がネットワーク上に残っていたりなどの軽微な異常がブラウザ上で即座に可視化されるのを目の当たりにしました。

利点

ITの内製化をかねてから推進しており、IT資産管理を徹底できている福岡ひびきだからこそ、Enterprise Immune Systemによってこのような脆弱性対策の漏れを包括的に確認できたことも踏まえて、実導入を開始した現在も投資対効果に見合っていると感じています。Enterprise Immune Systemは、教師なし機械学習を駆使して内部ネットワークの通信の定常状態を常時把握することで異常を検知するイノベーティブなアプローチを採用しており、従来のセキュリティツールでは全く顕在化しなかった脅威を一元的に可視化できるため、一時的に対応負荷が増加する実感があるものの、約1時間でインストールが完了することや、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が危険度によって自動的にアラートを上げるため、総じて運用効率が向上しました。

（※）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