社会医療法人恵仁会 様

社会医療法人恵仁会は、長野県佐久市・上田市周辺地域に医療福祉施設を展開し、医療部門は恵仁会の核となるくろさわ病院をはじめ、佐久市と上田市真田町、菅平高原に３つの診療所があります。また保健医学センターや健康運動センターが保健部門を担い、そして福祉部門では高齢者向け介護として３つの介護老人保健施設を中心にグループホーム、各種通所系サービス、訪問系サービスを充実させています。また、近年は障がい者、障がい児支援やスポーツ支援にも力を入れています。

社会医療法人 恵 仁 会

まとめ

- ✔ 医療機関を狙う高度なサイバー攻撃の増加に対する危機感
- ✔ 通信の定常状態学習とネットワーク完全可視化で従来対策をすり抜ける脅威を予兆レベルで検知
- ✔ 各アラートの異常度や因果関係まで AI が自動的に調査分析、少人数運用でも漏れなく対処

ネットワーク完全可視化で万一に備えたい

社会医療法人恵仁会（以下、恵仁会）は、「安心と安全に もっと 24 時間の愛情を」を理念に、地域に根付いた保健、医療、福祉の複合体として、1937 年の創業以来、地域の発展と歩みを共にしてきました。現在利用者から預かる 20 万件近くの個人情報と、2015 年に導入した電子カルテで保管する機微な医療情報を適切に保護するためのサイバーセキュリティ対策として、これまでは業務端末にシグネチャ型のアンチウイルスソフトを導入し、出入口対策として UTM（統合脅威管理）製品を活用し、主に境界で防御を固めてきました。

恵仁会では情報漏えいにつながりかねない深刻な脅威や通信異常が検知されたことはこれまでにありませんが、近年、国内外の病院や各種医療機関で境界型防御をすり抜けるランサムウェア攻撃など高度なサイバー犯罪による被害が未曾有の規模で拡大する中、万一実害を被った場合は機密情報の漏えいのみならず、最悪の場合は医療業務が停止に追い込まれる可能性も想定され、このような攻撃を未然に防ぐ対策を施すことは必要不可欠です。

恵仁会では、長野県内で運営する診療所などの各施設で現在合計 400 台弱のクライアント端末を日々の業務で利用していますが、洗練された標的型攻撃や未知の脅威を漏れなく早期に検知するためには、ネットワークの内部で業務端末の挙動や通信の状態を把握・可視化することが次のステップであるという認識の下、関連する次世代のセキュリティ製品の情報収集を進めていました。従来の境界型防御製品が検知できない不審なインバウンド通信や、ネットワーク内部の横方向の通信の状況、さらにアウトバウンドの通信も含め、恵仁会のネットワーク全体の生活パターンを丸ごと自動監視・完全可視化できる製品として、Darktrace Immune System の導入を検討しました。

「昨今、新手のランサムウェアが IT システムの不具合やファイル暗号化のみならず、病院内の基幹システムまで機能停止に追い込む実例が急増する中、シグネチャ型の境界防御だけでは太刀打ちできないという危機感がありました。平時の通信状態を機械学習する Darktrace の AI は従前から実現したかった内部通信の完全可視化に加えて、普段と異なる通信を漏れなく検知し、異常の原因まで自動調査できるため、少人数でも安心して運用できます。」

社会医療法人 恵仁会 経営企画課 林 嗣人 様

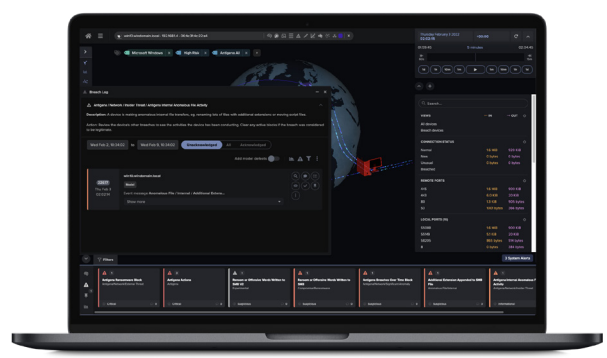
あらゆる通信異常をリアルタイムに把握

2021年8月、恵仁会がDarktrace Immune SystemのPOV（※）実施を決定した目的は、一義的にはネットワークレイヤーにおける通信を100%可視化する体制を整え、万一シグネチャベースの製品をすり抜けるサイバー攻撃の内部侵入を許してしまった場合も限りなく早期に把握・対処することですが、Darktraceがネットワーク全体の見える化を実現する技術の根幹には、独自の教師なし機械学習をベースにした通信異常のリアルタイム検知があります。

アプライアンス製品として提供されるDarktrace Immune Systemは、人間の免疫システムに着想を得て独自開発された自己学習型AIが、組織内のIPデバイス、ユーザーの普段の挙動や通信パターンを常に学習し、その時の定常状態から逸脱する「異常」をリアルタイムかつ自動的に検知し、アラートを発するものです。パケットキャプチャによりDarktrace Immune Systemがアプライアンス内で解析する要素は、通信の宛先や時間帯、通信量・通信頻度などが含まれます。ユーザー毎、デバイス毎、サブネット毎にこれらの要素を継続的・自律的に機械学習することでネットワークの普段の状態のベースラインを更新し続けるため、既存のルールやシグネチャに依存することなく、理論上いかなる未知の脅威や内部不正も検知・可視化することができます。オンプレミスのITネットワークに加えて、各種モジュールやセンサーを追加インストールすることでクラウド/SaaS環境、リモートワーク端末やIoT機器を含む組織のあらゆるデジタルインフラを全域にわたり網羅的に監視・自律防御できることも特徴です。

組織内の全トラフィックを機械学習する様子はウェブブラウザからアクセスできる独自の3D可視化ツール、Threat Visualizer上でリアルタイムに描画されます。定常状態からの逸脱度を客観的に示すしきい値をベースに、高異常度のアラートや端末、接続はThreat Visualizer上で自動的に色分けして表示されます。機械学習のメカニズムとしては、ITネットワークのコアスイッチに接続したアプライアンス製品がポートミラーリングによって業務端末と各種サーバー間のあらゆる通信パケットのヘッダー情報の収集・解析を行うのみで、恵仁会のデータセンターでインストール作業に要したのは1時間程度でした。

恵仁会では、POVの期間中に一度だけDNSサーバーがある電子カルテに対して不審な通信を行おうとしていたことをDarktrace Immune Systemだけが検知していたケースが発生しました。従来のUTM製品が見逃してしまったこのような脅威の芽の早期発見につなげるべく、2021年11月の実導入開始後は念には念を入れてしきい値を0%～100%に設定し、異常度の高低を問わず定常状態から逸脱するあらゆる通信異常をアラートとして自ら把握できるように運用しています。これにより、C＆C通信の可能性をリアルタイムに通知したり、あるいは業務に関係しないウェブサイトに対するアクセスの多寡をユーザー単位、デバイス単位で傾向として把握できるようになるなど、担当者1名の運用体制であっても網羅的に対策できている安心感があります。



Darktrace Immune Systemはルールやシグネチャに依存せず、事前設計やメンテナンスも不要ながら、いかなる未知の脅威や内部不正にも理論上、リアルタイムに自動対処できる唯一のサイバーAI技術を提供します。

アラートの自動調査・トリアージ機能で省力化

しきい値を幅広く設定しつつも、1名の運用体制で脅威対処の優先順位をつけられているのは、恵仁会でDarktrace Immune Systemに実装されているCyber AI Analystの機能を活用しているからです。Cyber AI Analystは、検知したアラートを人間のアナリストが人手で調査分析する際の数百万におよぶ思考パターンを数年間にわたり機械学習し続けたAIを実装し、AIが脅威調査までも高速自動化する世界初の技術で、検知したアラートの因果関係を平易な日本語で瞬時に文章化し、ワンクリックでPDFのインシデントレポートを自動生成できます。これにより、業務のすきま時間にブラウジングするだけでも異常の有無を漏れなく把握できるようになり、少人数の運用ながらこれまでにない安心感を得ることができました。

（※）Proof of Value：4週間の導入前検証。

詳細については以下をご覧ください

- 無償トライアルを申し込む
- Immune System ホワイトペーパーを読む
- Darktrace の YouTube チャンネル