DARKTRACE

医療法人 錦秀会 様

まとめ

- 近隣の病院に甚大な被害をもたらしたランサムウェアへの危機感と不安、未知のサイバー攻撃に対するより強固な多層防御を構築したい
- ミラーポートの設定のみでエージェントレス導入、チューニングも不要でシグネチャに依存しないAIが自律的に院内通信の定常状態を学習・可視化しあらゆる異常を検知・遮断。最小限の人手で漏れのない内部対策を実現

医療法人錦秀会（以下、錦秀会）は、大阪市南部・堺市・泉州・中河内・神戸市を医療圏とした2医療法人と1社会福祉法人、学校法人、公益財団法人、NPO法人から構成される錦秀会グループに属する西日本最大級規模の医療法人です。

対岸の火事ではないランサムウェアへの危機感と緊急対策

1957 年の阪和病院の開院から長い歴史を持ち、現在大阪市南部と堺市を中心に 5 病院 2 施設で総病床数 3,206 床を有する関西で屈指の規模の医療法人である錦秀会は、「やさしく “生命 (いのち)” をまもる」を理念に医療、介護、教育の複合機関として地域住民の健康を支えています。

錦秀会における従来のサイバーセキュリティ対策として、パターンマッチング型のアンチウイルス製品および多要素認証・接続先制限を行う VPN 製品の導入、データ退避・バックアップを目的とした各種 BCP 対策など、主に外部からのサイバー脅威に対抗する出入口対策や事後対策を入念に実施していました。

しかし、2021 年 10 月、徳島県の病院で電子カルテ情報やバックアップ用データが瞬く間に暗号化され医療業務遂行に甚大な影響が生じ、全国的にも大きく報道されたランサムウェア攻撃が発生した頃、錦秀会でも病院情報システムのリモート保守を目的として運用していた VPN 製品の脆弱性を突こうと試みる不正アクセスの回数が、従来の年間数十件ほどから 1 日あたり数百件と一気に急増し、最悪の事態を未然に防ぐためのより強固なセキュリティ対策が喫緊の課題であると認識するようになりました。

さらに、2022 年 10 月、錦秀会と同じく大阪市南部に拠点を置く急性期病院においてランサムウェアによる攻撃で医療業務が停止するという事案が発生し、いよいよ対岸の火事ではなくなってきたことから、情報系ネットワークのエンドポイントレイヤーにおける新たな NGAV（次世代型アンチウイルス）ソフトや EDR 製品の追加導入に並行して、ゼロデイ攻撃や未知の脅威を予兆段階で未然に検知する対策、さらに万一脅威の侵入を許してしまった際にネットワークの内部対策を効率よく実施できる NDR 製品で多層防御を重ねるべく、Darktrace 製品の POV（※）を開始しました。

他院でのランサムウェア攻撃の事案発生に呼応するように不正アクセスが急増したことに極めて強い危機感を感じていましたが、Darktrace の最先端の AI 技術により、今ではあらゆる脅威を予兆レベルで自律検知・遮断し、院内の全通信を完全可視化できるまでになりました。これまで積み重ねてきた多層防御への対策も含め、医療機関としては比較的進んだセキュリティ対策を構築できました。

/ 医療法人錦秀会 医事管理部
医事管理課 情報システム課 花坂 仁啓 様

医療法人 錦秀会

院内通信の完全可視化、異常の検知・遮断を AI が昼夜問わず自律実行

通常 HW/SW 一体型のアプライアンス型製品として提供される Darktrace の各製品は、ルールやシグネチャに頼ることなく、事前設計やメンテナンスも不要ながら、各組織に固有のユーザー・デバイスの挙動や通信の定常状態（生活パターン）を、独自開発の自己学習型 AI によりデジタルインフラの種類を問わず常時機械学習・完全可視化し、定常から逸脱するサイバー脅威をリアルタイムに自律検知・遮断、さらに検知した脅威の調査分析・日本語によるレポーティングまで高速自動化する世界初の技術に基づいて提供されています。オンプレミスの IT ネットワークに加えて、仮想アプライアンスや各種モジュール、センサーなどを追加導入することで、クラウド環境や各種 SaaS アプリケーション上の通信、リモートワーク端末、IoT 機器を含む組織のあらゆるデジタルインフラを網羅的に監視でき、通信の宛先や時間帯、通信量・通信頻度などをパケットキャプチャにより AI が常時解析し、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、学習した定常状態から逸脱するいかなる未知の脅威や内部不正も即座に検知・可視化します。

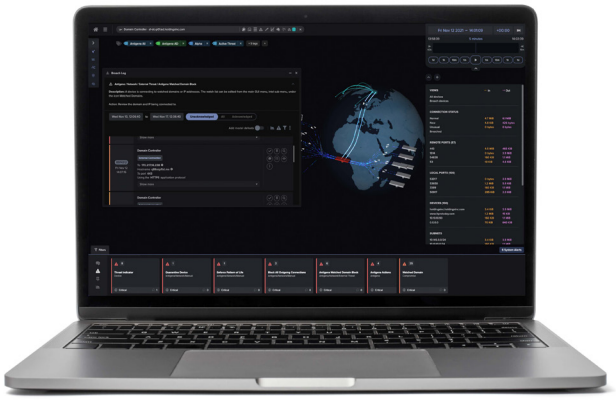
機械学習のメカニズムは、IT ネットワークのコアスイッチに接続したアプライアンス製品にミラーポートを設定することで業務端末と各種サーバー間のあらゆる通信パケットのヘッダー情報の収集・解析を行うというシンプルなもので、ウェブブラウザ上で閲覧できる Darktrace 独自の 3D 可視化ツールである Threat Visualizer が ネットワーク上を流れる通信パケットを一元的かつリアルタイムに描画を続けます。端末およびユーザーを示すアイコンや端末間の通信状況、また検知されたアラートは定常状態からの逸脱度を客観的に示すしきい値をベースに自動的に色分けして表示され、錦秀会では特に異常度の高い通信に対してリセットパケットの自動送出等により当該通信異常を 24 時間 365 日体制で自律遮断する製品、Darktrace/RESPOND も併せて導入しました。

Darktrace 製品はこのようにポートミラーリングによりエージェントレスで容易に導入できるため、錦秀会のデータセンターで実際にアプライアンスのインストールに要した時間は 1 時間程度でした。機密性の高い電子カルテ環境にアプリケーションを追加する必要なく、院内の医療機器やサーバーの通常稼働にも影響を与えることなく導入・運用が可能で、さらに閉域網における通信状況の監視や業務時間外における通信異常の遮断についても AI が自律的かつリアルタイムに実施するため、人手を最小限に抑えつつ死角のない対策を行うことが可能です。

2 名体制でも死角なきランサムウェア対策を実現

実導入後の 2023 年 11 月現在、錦秀会ではグループ全体で約 3,000 デバイスからなる病院情報システムにおける通信状況を Darktrace 製品で一元監視し、担当者 2 名での運用を実現しています。このような少人数運用を可能にしたのは、定常から逸脱した通信が発生した際のアラートを錦秀会では Microsoft Teams のメッセージとして即座に通知できるように設定し、Darktrace/RESPOND 専用のモバイルアプリで日時や担当者の居場所を問わず通信異常の自律遮断の実行モードを曜日や時間帯、異常度別に緻密に設定できる点が挙げられます。万一ランサムウェア攻撃の予兆が発生したとしても昼夜問わず最も早期に自律阻止できる体制を実現し、安心感が格段に向上しました。

（※）Proof of Value：4 週間の導入前検証。



Darktrace の各製品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