LANSCOPE Professional Service　DARKTRACE

医療法人 錦秀会 様

業種 医療・福祉
URL https://kinshukai.or.jp/
会社規模 3,828 名（2024 年 2 月時点）
事業内容 病院・施設の運営

AI 技術を駆使し、2 名体制で運用可能とした死角なきネットワークセキュリティ対策

西日本最大級規模の医療法人 錦秀会（以下、錦秀会）は、大阪市南部・堺市・泉州地域・中河内地域・神戸市を医療圏とする 2 つの医療法人と社会福祉法人のほか、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している。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、総病床数 3,206 床を有する関西屈指の規模の医療法人だ。「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る。

IT 資産管理として統合エンドポイントマネジメント「LANSCOPE エンドポイントマネージャー オンプレミス版」を導入済みで、今回新たに AI 型ネットワーク脅威検知「Darktrace」をご検討・ご導入いただいた背景を伺った。

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

「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 における最先端の AI・遮断することができるようになり、院内の全通信が完全に可視化されました。これまで積み重ねてきた多層防御への対策を含め、医療機関としては比較的進んだセキュリティ体制を構築することにより、IT-BCP の観点においてもリスクに対する被害の最小化につながり、且つ医療業務を中断させない為の対策を取ることができたと考えています。また一方でこれらの対策により、地域住民の方々にもより安心して受診していただける医療機関になったのではないかと考えています。」

――― 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 氏

選定のポイント

錦秀会では、以下の 3 つをポイントとして NDR 製品を検討し、「Darktrace」の採用を決定した。

1. 最も重要なことは、「医療従事者が安心して IT を利用できる」仕組み

まず、対策のために導入する新たなソリューションは、医療業務やシステムに悪影響を与えないことが大前提であると考えた。その点、Darktrace は、IT ネットワークのコアスイッチにアプライアンス製品を接続し、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を収集・解析する、というシンプルな製品だ。そのため、エージェントレスで容易に導入でき、院内の医療機器やサーバーの通常稼働にも影響を与えなかった。

2.「あらゆる侵入を逃さない」　網羅的に内部ネットワークを監視

また、病院全体のシステム構成や環境は複雑多岐にわたり、対策のためには「VPN 機器」や「関連組織のネットワーク」、「ベンダーの持ち込み端末」、「医療用 IoT 機器」など、あらゆる経路からの侵入を想定しなければならなかった。「想定される攻撃は PC などの端末を経由しないことも多く、エンドポイントの監視だけでは不十分です。患者様の診療情報という非常に機微な情報を含む電子カルテなどの重要システムを守るため、内部ネットワークを網羅的に監視する必要性を感じていました」と、錦秀会の IT コンサル・導入支援・運用保守を担当しているアスクラピウス株式会社の高島氏は話す。

これに対し Darktrace は、業務端末と各種サーバー間のあらゆる通信パケットをもとに解析を行うため、内部サーバーや業務 PC はもちろん、VPN や関連先からの通信も可視化できる。「AI が自己学習しているので精度が良いこと、また、インターネットとの通信を前提としない閉域網でも使えることが非常に嬉しい」とアスクラピウス株式会社の村尾氏は評価する。

3. システム管理者の運用負荷が少ないこと

そして、持続可能な運用のためには、管理者の負荷は徹底して抑える必要がある。

「多くの医療機関、あるいは企業・組織の担当者が悩まれているのと同じように、私達も、残念ながらセキュリティ運用に潤沢に人的リソースを割くことはできません。強力な助っ人が必要でした」と花坂氏は話す。

Darktrace 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で AI が常時学習するため、管理者の運用負荷を徹底的に軽減できる製品だ。

また、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などにより該当の通信異常を 24 時間 365 日体制で自律遮断する「Darktrace RESPOND」もあわせて導入している。これにより、運用負荷を掛けることなく、検知の次の「対応」のフェーズも自動化された。

導入の効果

導入から 5 ヶ月経過した現在、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の通信状況を Darktrace 製品で一元監視している。そして、それを担当者 2 名でという少人数運用を可能とした。運用上の工夫として、定常から逸脱した通信が発生した際のアラートを、Microsoft Teams のメッセージとして即座に通知されるように設定することで、Darktrace RESPOND 専用のモバイルアプリで、時間や担当者の居場所を問わず、通信異常時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操作できるようにしている点も挙げられる。

最後に、花坂氏は「今後、万が一、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構築できたことは錦秀会グループにとって大きく、担当者である私達も、何より医療従事者達も安心感が格段に向上した。

エムオーテックスとはセキュリティ診断などでも連携し、今後もさらなるセキュリティ強化を一緒に進めていきたいと思っている。引き続き手厚いサポートや有用な情報提供を期待している」と述べ、締めくくった。

※本事例は 2023 年 11 月取材当時の内容です。

アスクラピウス株式会社

IT コンサル・導入支援・運用保守
アスクラピウス株式会社
会社 URL：https://asclepius.co.jp/

●開発／販売
エムオーテックス株式会社

本 社	〒 532-0011 大阪市淀川区西中島 5-12-12 エムオーテックス新大阪ビル　TEL：06-6308-8980
東京本部	〒108-0073 東京都港区三田 3-5-19 住友不動産東京三田ガーデンタワー 22階　TEL.03-3455-1811
名古屋支店	〒 460-0003 名古屋市中区錦 1-11-11 名古屋インターシティ 3F　TEL：052-253-7346
九州営業所	〒 812-0011 福岡市博多区博多駅前 1-15-20NMF 博多駅前ビル 2F　TEL：092-419-2390

TEL：03-5460-1372 受付時間 9:00-18:00（月～金曜日）
E-mail：sales@motex.co.jp　URL：www.motex.co.jp

お問い合わせ先