

愛生館グループ

CrowdStrike Falcon® (クラウドストライクファルコン) プラットフォーム / GSXアラート監視サービス

「高度な脅威に対する検知力、未知の脅威に対する抑止力、端末に負荷が掛からない等の観点から検討しましたが、何より導入コストやGSXのサービス体制の盤石さから導入を決定しました。」

愛生館グループのご紹介

愛生館は、愛知県の三河地方でおよそ75年にわたり、地域のセーフティーネットとして事業を行ってきました。現在は、拍車のかかる超高齢社会を支えるため、地域包括ケアシステムの更なる深化に向け、グループ全体で様々な事業（医療・介護・福祉事業）に取り組んでおります。

愛生館では「地域で生活している子どもから高齢者まで誰もが安心して暮らせる地域づくり」を目指しています。

少子高齢化や人口減少という社会的課題は、これから我々の生活を更に大きく変化させていきます。このような時代だからこそ、地域の人と人が繋がる必要があります。これからも、愛生館はこの地域にある行政、企業、事業所等の様々な方々と共に「0歳から100歳までの方々を支援する仕組みづくり」を追求し続けます。

そして、「人々の人生をより豊かにする」という使命に基づき、地域の方々に「愛生館があって良かった」と思っていただけのように、社会的課題に対して更なる努力を重ねてまいります。

導入のきっかけや背景をお聞かせください

電子カルテとは別ネットワークの事務環境で利用している端末1台でEmotet（エモテット）感染が検出され、グローバルセキュリティエキスパート（以下、GSX）にフォレンジック調査を依頼しました。事務環境のセキュリティ強化が重要課題であったことも併せ、再発防止策としてエンドポイントセキュリティをご提案いただき、導入に至りました。

導入以前は社内にどのような課題があり、どのような解決策を検討したのかお聞かせください

電子カルテ環境はネットワーク隔離されており安全性も確保しておりました。かたや事務環境ではセキュリティ全般について脆弱であることを認識していました。まず、恒久対策として端末を保護し、防御力を上げるためにエンドポイントセキュリティの導入を急ぎました。

今回の対策でエンドポイントセキュリティ強化ができましたので、あらためて課題を整理し、順次セキュリティ強化を進めていきます。



医療法人 愛生館 小林記念病院
統括本部 総務部
情報システム担当課長

近藤 知之 氏

愛生館グループ

■所在地

愛知県碧南市・安城市

■関連施設

小林記念病院(196床)、介護老人保健施設、特別養護老人ホーム、小規模多機能、訪問看護、通所介護、認定こども園など

■従業員数

1,048名
(2023年7月現在)

■代表

小林清彦

CrowdStrike Falcon® (クラウドストライクファルコン) プラットフォームとは

CrowdStrike Falcon プラットフォームは、クラウドに収集された全世界の端末の振る舞いログを監視し、高度なサイバー攻撃をリアルタイムに判断・検知する統合セキュリティプラットフォームです。

CrowdStrike Falcon プラットフォームは、従来型のマルウェア攻撃の防御に加え、優れた機械学習と人工知能、振る舞い分析により、ファイルレス攻撃などの高度な脅威を検知・抑止することで、お客様のエンドポイントを保護します。

クラウドストライク製品には、CrowdStrike Falcon Prevent (NGAV)、CrowdStrike Falcon Insight XDR (EDR/XDR)、CrowdStrike Falcon OverWatch (マネージド脅威ハンティング)、CrowdStrike Falcon Spotlight (脆弱性管理)、CrowdStrike Falcon Discover (IT資産管理) および CrowdStrike Falcon Cloud Security (CNAPP) などが含まれます。

またGSXではCrowdStrike Falcon プラットフォームの製品運用をご支援する「MDRサービス for CrowdStrike Falcon」というMDRサービスをご提供しております。

セキュリティ対策について 今後の展望をお聞かせください

CrowdStrikeの機能には満足しています。運用面で端末入替時のシームレスな移行が課題です。標準で自動機能があると助かりますね。できれば同業他社の(成功)事例を参考にしたいと考えています。昨今、ChatGPTなどの生成AIがもてはやされていますが、当該機能を活用した自動化や効率化には非常に興味があります。

今回、エンドポイントセキュリティ強化による検知/抑止/防御力向上が実現できました。コンピューターシステムでのセキュリティ強化は当然として、従業員の意識向上のため、教育も充実していきます。医療法人ではPマーク取得についても検討しております。



医療法人 愛生館 小林記念病院

他社サービスを検討しましたか

複数の著名なエンドポイントセキュリティ製品を検討しました。導入後のメンテナンス性や、運用管理する上での懸念を払拭できる製品を選定しました。

CrowdStrike Falconプラットフォーム製品採用のポイントや決定打はどのようなところでしたか

高度な脅威に対する検知力、未知の脅威に対する抑止力、端末に負荷が掛からない等の観点から検討しましたが、何より導入コストやGSXのサービス体制の盤石さから導入を決定しました。

効果・効用をお聞かせください

製品導入後、ウイルス検知のアラートが上がることもあり、防御/抑止を明示的に認識できるので以前と格段に違う安心感があります。効果の見える化が実現できています。

CrowdStrike Falconプラットフォーム 導入前の主な課題や問題点

セキュリティ全般対策

- ・ウイルス検知の仕組みが多層的ではなかった
- ・従業員へのリテラシー教育の必要性

高度な脅威や未知の脅威に対する態勢

- ・高度な脅威に対して早期に検知できること、未知の脅威(ウイルス)に対する確実な抑止を実施できること

CrowdStrike Falconプラットフォーム 導入による効果・効用

- 高度な脅威に対する検知力、未知の脅威に対する抑止力、端末に負荷が掛からない、加えてGSXのサービス体制の盤石さがあった
- ウイルス検知のアラートが上がると防御/抑止を明示的に認識できるので以前と格段に違う安心感がある、効果の見える化が実現できている

お問合せ

GSX
GLOBAL SECURITY EXPERTS

グローバルセキュリティエキスパート株式会社

〒105-0022 東京都港区海岸1-15-1 スズエベイディアム4F
☎ 03-578-9001 ✉ sales-all@gsx.co.jp