

急増するサイバー攻撃防御の自動化に！

大規模な医療機関(米国)が、CleanINTERNETサービスを導入することで、日々6,000万件あったイベントログを50万件に激減！

課題

大規模な研究病院では、人々が研究、業務、ケアを継続的に行えるようにすることが課題となっています。同時に、ネットワーク、データ、デバイスを危険にさらすことなく、必要なツールやプロセスに安全にアクセスできるようにする必要があります。

病院のシステムは、インフラが構築されていくにつれて、テクノロジーにますます依存するようになり、デリケートな病院のエコシステム内の患者ケア、研究、請求などの部門は、サイバー攻撃など外部からの脅威によりさらされることとなります。これは、データやネットワークのセキュリティだけでなく、患者の生命そのものを危険にさらすこととなります。

1万人以上の従業員と年間150万人以上の外来患者を抱えるこの医療機関では、守るべきものがたくさんあります。

この大規模医療機関では、ファイアウォールで1時間に300万件、毎日合計で6,000万件以上のイベントが発生していました！

解決策

同医療機関は、Centripetal Networks社と協力し、プロアクティブなソリューションであるCleanINTERNETサービスを導入しました。

包括的なサービスであるこのソリューションは、ネットワークを事前に保護するので、効果的に動作しながら、医師、患者、研究者、スタッフ、または医療機器など多様な環境に対して高いレベルの保護を提供します。

「ファイアウォールのログを抜き打ちチェックした所、CleanINTERNETサービスを導入する前は6000万件/日あったイベントログが、先日は50万件まで減少していました！」

- 北東部大規模医療機関
(シニアサイバーセキュリティアーキテクト)



結果

最適な状態に至るためのシールドリング(ブロッキング)の工程において、最初の1日で、一日を通しての(ファイアウォールでの)ブロック件数が402,000件になりました。
その後、さらに追加でサイバー脅威インテリジェンスフィード(脅威データ)を適用したところ、一日を通してのブロック件数が213,000件に減少しました。

“当初、1時間あたり300万件のブロックだったのが、1時間あたり2万件のブロック、1時間あたり6,000件のブロックと減っていきました。
現在、3週間かけてインバウンドトラフィックイベントのブロックをSIEMに記録していますが、その量は以前、1時間でSIEMに記録していたブロック量です。”

- 北東部大規模医療機関
(シニアサイバーセキュリティアーキテクト)

この医療機関では、ファイアウォールで記録されたインバウンドトラフィックイベントのブロックをSIEMで測定しています。
SIEMは保存に費用がかかるため重要です。通常のファイアウォールブロックメッセージサイズは2KBとすると、1時間あたり5.7GB保存していたのが、1時間あたり11.7MBになり、大幅なコスト削減を実現しました。

2ヶ月後、信頼度の高い脅威を数回シールド(ブロック)しただけで、CleanINTERNETサービスの導入に関連したネットワークの障害報告はゼロでした。

CentripetalのCleanINTERNET®サービスは、大規模かつ高速に動作し、世界の脅威情報(Threat Intelligence)コミュニティによって特定されたほぼすべての既知のサイバー脅威からお客様のビジネスを動的に保護します。

**まずは1ヶ月間の無償トライアルで導入効果を御確認ください！
【お申し込みは御電話もしくは<https://www.cornet-solutions.co.jp/contact/>にて！】**

日本総代理店

コーネットソリューションズ株式会社
 (TEL) 03-5817-3655(代)
www.cornet-solutions.co.jp

— [Centripetal Networks社は北米企業の成長率ランキング「Deloitte's 2021 Technology Fast 500」にランクされています](#) —