

BROMIUMがMOFFITT がんセンターの コンピュータネットワーク の保護に貢献



H. Lee Moffitt がんセンター & 研究所は、フロリダ州タンパにある非営利のがん研究・治療施設です。Moffittは、米国国立がん研究所が指定した49の総合がんセンターの1つであり、全米で第9位のがん専門病院にランクされています。1999年以降、MoffittはU.S. News & World Report誌で、がん治療に最適な病院のひとつにリストされています。



Moffitt がんセンターが評価されているのは、優れた研究と優れた患者ケアだけではありません。2017年には、Moffittの最高情報セキュリティ責任者であるDave Summitt氏がInformation Security Executive Southeast People's Choice Awardを受賞し、配下のセキュリティオペレーションセンター（SOC）がリーディングプロジェクトにノミネートされました。Summitt氏は、国防総省に21年間勤務した後、ヘルスケア分野に転身した業界のベテランです。過去13年間は、特にサイバーセキュリティに注力し、フィッシング攻撃やランサムウェアなどの脅威から病院のコンピュータシステムを守るために活動してきました。

放射線機器のセキュリティ確保

「医療機関では、放射線部門のセキュリティ確保が最も困難な分野の一つです。そして、パフォーマンスに影響を与えないセキュリティ・ソリューションを見つけることが特に重要です。」とSummitt氏は言います。「画像は非常に詳細である必要があり、医師は通常、一度に複数の画像を見ることを要求し、これらの情報をリアルタイムで必要とすることが多いのです。」放射線スキャンやその他の医療画像を読影するマシンは、GE-PACSが動作する通常のWindowsベースのワークステーションです。これらのマシンはネットワークに接続されており、職員がこれらのマシンを使って電子メールをチェックしたり、インターネットを閲覧したりすると、Web経由のマルウェアや悪意のあるEメールの添付ファイルに潜む脅威にさらされる可能性があります。

しかし、Summitt氏のチームがアンチウイルスソフトウェアを導入してみたところ、パフォーマンスが大幅に低下するという問題が発生しました。「画像が送られてくると、アンチウイルス・ソフトが画像を拾い、脅威がないかスキャンしてからビューワに表示するのです。」とSummitt氏は説明します。「これでは本当に遅くなってしまいます。」Moffittのセキュリティチームは、既知および未知の脅威からマシンを保護しつつ、操作性とパフォーマンスを維持できるソリューションを見つける必要がありました。

Bromiumの新しい使い方

Summitt氏は、アラバマ大学のBirmingham Healthcare SystemでCISOの役職に就いていたとき、初めてBromiumを知ったことを思い出しました。「最初に提示されたときは、まさに"WOW"の瞬間でした。初めてBromiumを見たその日に、私はBromiumに恋をしたのです！」と語ります。

Moffittに移ったSummitt氏は、自分の環境に潜む可能性のある潜在的な脅威をよりよく理解するためのツールとして、新しいセキュリティ組織にBromiumを導入しました。

チームは当初、Bromiumを使用して少数の選択したPCを意図的に感染させ、そのライフサイクルを通して脅威がどのように展開し、どのように振る舞うかを観察しました。Bromiumの完全なキルチェーン分析は、脅威に関するすべての利用可能な情報を収集し、そこから学び、Moffittのサイバー防御を強化するのに役立ちます。

「そして、私はあることに気がつきました。」Summitt氏は続けます。「我々はすでにBromiumを所有しているので、放射線機器からアンチウイルスを取り除き、代わりにBromiumで保護することを試みてはどうだろうか。」最初のトライアルは成功し、現在では30台以上のMoffittの重要な放射線読影マシンがBromiumを搭載しています。

「インターネットからファイルをダウンロードしたり、Eメールをチェックするなど、放射線治療とは関係のない目的でこれらのマシンを使用している人がいても、我々には保護する方法があります。」とSummitt氏は結論づけています。

実際の節約と目に見えるパフォーマンスの向上

放射線科のワークステーションのアンチウイルスをBromiumに置き換えて、Moffitt氏はマシンのパフォーマンスが大幅に改善されたことに気がきました。

最新のコンピュータスキャン機器は、患者の体の大部分の写真をわずか数秒で撮影できるように設計されています。しかし、ウイルス対策のために画像読取装置の動作が遅くなり、Moffittの放射線科医や技術者は、各スキャンが表示されるまで数分待つことも珍しくありませんでした。

この遅延が、コストと患者ケアの効率化の大きな要因であることが明らかになりました。この遅延をなくすことで、スタッフの生産性が向上し、医師が患者の治療に関する意思決定を迅速に行えるようになり、医師の満足度も高まります。

Summitt氏は、BromiumがMoffittのITセキュリティとSOC業務を合理化したと評価しています。Bromiumを使用することで、セキュリティ・オペレーション・チームは、入ってきたマルウェアの影響を迅速かつ効率的に判断し、より大きな問題になる前に緩和対策を開始することができます。

Bromiumユーザーを拡大する

アンチウイルスを排除することは、どのような組織にとっても、特に大規模なヘルスケア施設にとっては真のパラダイムシフトを意味しますが、Summitt氏は、彼のチームがすぐにその障壁を打ち破り、Bromiumでより多くのエンドポイントを保護できるようになると楽観的に考えています。彼の当面のターゲットは、VPNでセンターのネットワークに接続するMoffittのリモートワーカーです。「アンチウイルス・ソフトウェアをアップデートして、それをリモート・ユーザーにプッシュするという問題が常にあります。」と彼は説明します。「私の次の目標は、リモート・ユーザーのエンドポイントからAVを取り除き、Bromiumで置き換えることです。」

他の医療機関との経験の共有

今日の医療施設のほとんどは放射線画像を読み取る機械を使用しており、Moffittが遭遇したのと同じ問題を経験している可能性も多いでしょう。これらの機器は保護されていない状態ではいられませんが、アンチウイルスによってパフォーマンスの問題が発生します。特に患者の治療に関する迅速な決定を行うためにスキャン画像を素早く読み取る必要がある場合に、これは受け入れられません。Summitt氏は、Bromiumを放射線機器に使用したチームの経験を他の病院と共有し、重要なテクノロジーを最適な状態で稼働させるためのセキュリティアプローチの構築を支援することを計画しています。

2020年5月にHP Inc. により再リリース

