CrowdStrike 導入事例

アステラス製薬株式会社

世界70カ国1万数千台のPCに CrowdStrike Falcon®を展開

脅威の正確な可視化と意思決定の半自動化で、“眠れる日々”がCSIRTに

世界約70カ国でビジネスを展開する日本発のグローバル製薬企業

アステラス製薬株式会社は、世界約70カ国でビジネスを展開する日本の代表的なグローバル製薬企業だ。「変化する医療の最先端に立ち、科学の進歩を患者さんの価値に変える」をビジョンとし、「患者志向」、「主体性」、「結果」、「多様性」、「誠実」という5つのグループ共通のAstellas Wayを世界中のアステラス社員が共有する。

がんや泌尿器分野の医薬品開発に定評があり、なかでも XTANDI／イクスタンジは米国、欧州、日本、アジアなどで前立腺がん治療剤としてトップブランドとなっている。他にも、過活動膀胱治療剤 ベタニス／ミラベトリック／ベットミガといった主要製品があり、成長をけん引する新薬の育成と製品価値の最大化に注力し続けているのが大きな特長だ。

侵入を前提とした検知と対応を情報システム部門CSIRT主導で実現したい

同社では、リスクマネジメントを重視している。その中でも最重要リスクととらえる対象の一つがサイバーセキュリティだ。アステラス製薬株式会社 情報システム部長 須田真也氏は、次のように語る。

「アステラスが大切にしているのは、医薬品を患者さんに適切に届けること、正しい情報を医療従事者に届けることです。システムがきちんと動き、信頼できなければ、これら2つのミッションを遂行できないということを経営層も強く認識しています」

そのため、情報システム部門を中心に、ネットワークおよび設備の監視を始めとする各種サイバー攻撃対策を、グローバルベースで実施し、その管理には万全を期している。実際、アステラス製薬の海外事業体制は拡大の一途をたどっている。今や日本以外の地域の売上比率は約70%、日本以外の地域の従業員比率も約65%に達していることから、同社は実績ある海外事業者にSOC運用をアウトソーシング、情報システム部をはじめとする社内のCSIRTと密接に連携しつつ、日々のオペレーションを行っている。

エンドポイント保護という観点では、端末環境のシンプル化という観点から近年はWindows Defenderを活用していたが、情報システム部門内ではアンチウイルスソフト以上の対策が必要だという認識が2017年ごろから強まっていた。マルウェアの形状を取らない脅威も増え、シグネチャーベースのウイルス対策には限界がある。そのため侵入されることを前提として、検知して対応するEndpoint Detection and Response（以下、EDR）の体制を強化すべき、それも情報システム部門がイニシアチブを取って対応できるような形で実現すべきと考えたのだ。須田氏は、次のように語る。

「私たちにはSOCチームがありますから検知は可能です。しかし、正しい対応のためには、今何が起こっているかを正確に知るビジビリティ（可視性）が必要です。私はセキュリティインシデントを山火事と同じだといっています。煙が発生し火がついてしまったら、その火を追いかけるだけでは消火は不可能です。火の回る方向を予想し、『この木とこの木を伐採して火を止めなさい』という的確な指示を出さなければなりません。SOCチームからの報告だけでは全容がつかみにくかったきらいがありました。

また検知できるだけでは不十分であり、結局、次に取るべきアクションを判断するのは人間になります。グローバルでビジネスを展開している当社にとって、意思決定者は24時間365日対応をせざるを得ないのも問題でした。そもそものスタートとして、『CSIRTがちゃんと眠れる仕組みを考えましょう』と声をかけた記憶があります」

その当事者といえるのが、まさにサイバーセキュリティグループリーダー 次長 高草木泰彦氏だった。SOCチームからいつ連絡が来てもいいように、携帯電話は肌身離さず持参していた。また、夜寝入ってからもインシデント対応状況が気になり、深夜に目を覚ましてしまうなどいつも心が休まらない状況だったという。

業種
製薬

所在地
東京都中央区日本橋本町2-5-1

アステラス製薬株式会社

先端・信頼の医薬で世界の人々の健康に貢献する「日本発のグローバル製薬企業」になるという経営理念の下、山之内製薬と藤沢薬品工業が合併して誕生した。2005年の発足以来、イノベーションを継続的に創出し、患者のニーズに応える革新的な医療ソリューションを届けるという一貫した姿勢でグローバルに事業を拡大しながら着実に歩み続けている。

URL：https://www.astellas.com/jp/ja/

導入製品
- CrowdStrike Falcon Insight™ EDR
- CrowdStrike Falcon OverWatch™ 脅威のハンティング
- CrowdStrike Falcon Prevent™ 次世代アンチウイルス

導入時期：2019年11月

クラウドプラットフォームという製品コンセプトを高く評価して採用

同社とCrowdStrike Falcon®との出会いは、2018年だった。評価の高さから本命視し始め、グローバルベースで導入するに値するかという観点などさまざまな観点で検討し、採用を決定した。高草木氏はその理由を次のように語る。

「CrowdStrike Falcon®の製品コンセプトに惹かれました。クラウドネイティブのプラットフォームであり、当社のみならず世界中のクラウドストライクユーザーのすべてのインシデントや対応ナレッジがそこに集約され、地球の裏側で起きた新しい攻撃への対策が、次の瞬間には日本でも可能になるという点がよかったですね。

また、クラウドストライクは自ら調査や分析を行い、豊富に脅威インテリジェンスを有しているところも高く評価しました。その結果、当初はEDRという観点からCrowdStrike Falcon Insight™の検討を進めましたが、人の目で脅威ハンティングを行うCrowdStrike Falcon OverWatch™もよいということになり、既存のアンチウイルスソフトでは検知できない脅威を検知可能な次世代アンチウイルス CrowdStrike Falcon Prevent™も合わせて導入することにしました」

須田氏は高草木氏を補足してこう語る。

「パッケージ製品が主流だった時代は機能比較をしたものでしたが、クラウドサービスとなると現時点の機能を詳細に比較することに意味はありません。数か月も経てば状況は大きく変わるからです。そこで私たちが注目したのが『製品コンセプト』『将来性』で、5年後、選択に間違いはなかったと思えるか、という観点で検討したら、この製品になったということだと思います」

脅威のビジビリティ（可視性）を得てピンポイントで効果の高い対応が可能に

導入を開始したのは2019年11月のことだった。支給しているノートPCのリプレースタイミングに合わせて日本の事業拠点から展開し始め、現在ではグローバルの全事業拠点の1万数千台のエンドポイントでCrowdStrike Falcon®が稼働している。

スタート時は、アンチウイルスソフトも併用されていたが、端末環境をシンプルに保ちたい意向もあったため、CrowdStrike Falcon Prevent™に一本化された。

現在、CrowdStrike Falcon®の管理コンソールをSOCチームとCSIRTで共有しており、日々のオペレーションはSOCチームが行うものの、いつでも自社メンバーが状況を確認できる。また、インシデントが発生した際、その緊急度が「High」であれば、指示がなくてもSOCチームの判断で該当のエンドポイントを停止できる運用体制を整備した。これは同社ならではの意思決定の半自動化ルールである。システムDR（災害復旧）対策でも、自然災害などで東日本のシステム系統に障害が発生した際、事前に定めた条件が揃えば指示がなくても西日本のシステム系統にスイッチしてよいという方針が確立されており、それが踏襲された形だ。

CrowdStrike Falcon®を導入して何が変わったか、という問いに、須田氏はこう答えた。

「SOCチームからの報告に頼りすぎることなく、自らファクトをつかみに行けるようになったことは大きいですね」

高草木氏が続ける。

「CrowdStrike Falcon Insight™でビジビリティを得たことは、確かに大きいと思っています。脅威がどう侵入してきて、エンドポイントの中で何をしようとしているか、次にどう動こうとしているかといったことがはっきり見えるようになったことで、ピンポイントで効力の高い対抗策を取れるようになりました」

また、CrowdStrike Falcon OverWatch™に関しても、侵入の兆候を捕捉し、緊急対応で事なきを得たこともあったようだ。

そして何より、高草木氏には深く眠れる日々が戻ってきた。深夜に何が発生しても、SOCチームで検知からエンドポイントの隔離まで一連のオペレーションを行えるようになったため、同氏は朝起きてから隔離の解除を判断すればいいだけになった。

今後は数千台のサーバにCrowdStrike Falcon®を展開

同社では今後、サーバ群に対してもCrowdStrike Falcon®を展開することをすでに決定している。須田氏は語る。

「全方位のビジビリティを確保しようと思えば、サーバを欠かすことができません。何かあればエンドポイント以上に被害の拡大するのがサーバというのもあります。サーバはエンドポイント以上に追加モジュール導入の“お作法”が難しいのは確かですが、当社は情報システム部門がすべてのサーバを統括している強みを生かし、これを進めていきます」

また、情報システム内CSIRTの、グローバルベースでのさらなる検知対応能力向上も重要なテーマとされている。

「ツールは入れて終わりではなく、そこからが始まりです。いかに使いこなすか、いかに効果的に使うかを考えながらさらにスキルやナレッジを磨いていきたいと考えています」

高草木氏はこう語りながら、次なる防御ステージを見据えていた。

アステラス製薬株式会社
情報システム部長
須田 真也 氏

アステラス製薬株式会社
情報システム部
サイバーセキュリティグループリーダー
次長
高草木 泰彦
CISSP

POINT

- サーバーを含めエンドポイントにFalconを導入、正確なビジビリティ（可視性）を確保
- クラウドプラットフォームが、グローバル運用を可能とし、企業のグローバル化を支える
- CrowdStrike Falcon®の管理コンソールで、外部SOCの報告を待たずに、自ら状況の確認が可能
- リモートでも対応が可能になり、レスポンススピートも早く、正確に

CROWDSTRIKE

we stop breaches

クラウドストライク 株式会社
お問い合わせ: **crowdstrike.jp/request-information/**