voices

CrowdStrike 導入事例

バリュエンステクノロジーズ株式会社

運用こそがセキュリティの核心
専門性を最重視しクラウドストライクのMDRを選択

Valuence
Circular Design Company

グループIT強化の一環で、まず次世代アンチウイルスの導入を決定

昨今、世界各国でカーボンニュートラルや環境保護といったサステナブルな社会形成が提唱されている。そうした中、国内におけるブランド品や貴金属、骨董・美術品等のリユース事業をメインに成長を続け、循環型社会の一端を担っているのが、バリュエンスホールディングス株式会社だ。経営トップは元プロサッカー選手の嵜本晋輔氏。グループ傘下で、ブランド買取専門店「なんぼや」「BRAND CONCIER」や骨董・美術品の買取専門店「古美術 八光堂」などを展開している。

このバリュエンスグループのIT部門を担っているのが、バリュエンステクノロジーズ株式会社である。同社は、グループのシステム開発を企画からインフラ構築、業務システム設計・開発、AI開発まで包括的に手がけている。この開発力を生かし、AIエンジンの構築だけでなく業務に活用していくためのDB再設計、組み込み開発の外販も行っている。

近年、バリュエンスグループは業容拡大を続けており、経営トップは成長に合わせ、グループITおよび情報システム部門機能の強化を決断した。その牽引役は、バリュエンステクノロジーズ 執行役員CIOおよびコーポレートIT部 部長 木戸　啓太氏だった。グループIT強化のため、ITの上流から下流まで課題を洗い出し、リスク分析を行いITロードマップを策定した。もちろんセキュリティ分野も例外ではなかった。当時、エンドポイント保護に関しては、グループではWindows OS標準搭載のウイルス対策ソフトを利用していた。同グループには約2割ほどMac OSも存在したが、この端末に関しては特に対策は講じられていなかった。これでは未知のマルウェアに対処することはできないと、2020年1月、クラウドストライクの次世代アンチウイルス製品であるCrowdStrike Falcon Preventの導入を決定した。すでにこの時にはEDR導入を見据えており、導入前の製品選定の検証には、次世代アンチウイルスに加えEDR製品であるCrowdStrike Falcon Insightも含めていた。

なぜクラウドストライクを選択したのか。それは木戸氏がこれまでのキャリアで幅広いエンドポイント保護製品を活用し、そうした中でふるまい検知機能を持つクラウドストライク製品が優秀であることをすでに認識していたからだ。それでも今回の導入に際しては、あらためて機能検証を行い、その上での選択だった。同氏は理由を次のように語る。

「クラウドストライクのUIはわかりやすく、攻撃を受けた際のプロセスの動きなどもリアルに把握できます。また、端末にインストールするセンサーからリアルタイムに多くのコンピュータ情報が取得できるのもいいと思いました。さらに、CrowdStrike Falcon OverWatchという人による脅威ハンティングがあり、最近ますます巧妙化している攻撃もしっかり検出してくれます。攻撃者情報をクラウドストライクは持っているので、万が一攻撃者に関する攻撃を検知した場合にはそれが知れるのも良いと思いました。加えて、第三者機関や口コミの評価も高かったこともあり、確信を持って選択しました」

EDR運用における正しい運用とは何かを考え、ベンダーが提供するMDRを採用

EDRを導入することは決めていたが、考えるべきことに運用体制があった。木戸氏はここで、既存の情報システム部員をアサインするのはリスクがあると考えた。セキュリティ分野は専門性が高く、付け焼刃のスキルやナレッジでは十分な対応ができないのは目に見えていた。「セキュリティ専任エンジニアを雇ってはどうか」という話は出た。しかし、セキュリティ人材は市場でも不足ぎみであり、確保するなら人件費として1人当たり1,000万円以上、3人なら3,000万円以上はかかるという試算が出た。それならば外部の運用専門サービスを、コストパフォーマンス高く活用できるのではないかとの結論になった。

では、専門サービスをどのように選択するか。ここでも木戸氏が重視したのは、スキルやナレッジの専門性だった。検討の末に導

業種
システム開発事業、その他関連事業

所在地
東京都港区南青山五丁目6番19号
MA5

バリュエンステクノロジーズ株式会社

「提案力とテクノロジーで、あるがままに生きられる世界を創る。」をビジョンに掲げるバリュエンステクノロジーズ株式会社は、バリュエンスグループ各社に対するシステム・アプリ開発経験を通じて培った知見・技術を活用し、AIやDXの活用・推進に関するソリューションを提供する情報サービス会社だ。主なサービスに、「丸投げAI導入パッケージ」「情報システム部門特化型コンサルティング」がある。

URL：https://www.valuence-t.com/

導入製品

- CrowdStrike Falcon Complete™ Managed Detection & Response (MDR)
- CrowdStrike Falcon Prevent™ 次世代アンチウイルス
- CrowdStrike Falcon Insight™ EDR
- CrowdStrike Falcon Discover™ IT資産管理
- CrowdStrike Falcon OverWatch™ プロアクティブな脅威ハンティング

導入時期：2020年1月

入することにしたのは製品を提供しているベンダーであるクラウドストライクが提供するMDR(Managed Detection and Response)であるCrowdStrike Falcon Completeだった。

Falcon Completeは、エンドポイントにおける侵害を防ぐための必須要素製品を網羅している。具体的には、Falcon Prevent（次世代アンチウイルス）、Falcon Insight（EDR）、Falcon Discover（IT資産管理）、Falcon OverWatch（プロアクティブな脅威ハンティング）というクラウドネイティブで構築されたCrowdStrike Falcon プラットフォームから提供される4つのモジュールがここに包含されており、Falcon Completeチームが顧客に代わってすべての対応を担う。モジュールの管理・運用から、リアルタイム監視、検知に対する調査および対処まで全ての対応を行う。顧客と役割を分担することはない。これにより、必要なスキルと専門知識が顧客側に提供され、顧客側ではインシデント対応所要時間が短縮される。

「CrowdStrike Falconプラットフォームをベースにした MDRを提供するサービスは数多く存在しますが、自社製品を使って、製品に精通したセキュリティのスペシャリストがすべての対応を担ってくれるというならそれに優るものはない、それしかないと考えました。情報力がもう絶対的に違うだろうと思います。また、私たちが対峙する脅威を考えると、対応の一部を託すというのではなく、主導権を持ってもらった方が賢明だと判断しました。

選んだ理由はもう1つあります。スキルトランスファーです。Falcon Completeを契約することで、スペシャリストに相談ができるようになり、私たち自身もノウハウやスキルを獲得できます。私たちはクラウドストライクの力を借りて成長したいと考えました」

木戸氏は、Falcon Completeを採用した理由をこのように語る。

海外含め鉄壁の守りを実現、
社内エンジニアのスキル向上効果も

Falcon Completeの運用を開始したのは、2020年12月のことだった。現在は、バリュエンスグループのエンドポイント端末約1,000台がFalcon Completeでカバーされている。このうち約200台がMac環境だ。また、1,000台のうち70台は、米国や香港、シンガポールなど海外拠点に設置された端末である。

同社では木戸氏をリーダーとする5名の情報システム部員がFalconのコンソールへアクセスするが、Falcon Completeチームとのやりとりは、メールベースで行われている。少し緊急度の高いアラートの状況についてFalcon Completeチームから確認依頼があると、木戸氏の指示でチームが従業員へのヒアリングを行うなどの対応をする。導入当初はアラートも多かったが、Falcon Completeチームが運用しながらそれらを潰しているため、現状そのようなケースは月に1件あるかないかだそうだ。基本的にはFalcon Completeチームがすべて対応する。

導入からほぼ1年、Falcon Completeチーム利用のメリットを、木戸氏は以下の様に挙げている。

1. セキュリティエンジニアを新たに雇用せずに運用開始でき、費用対効果も高い。
2. 間接コストを抑えることができる：何かインシデントが発生したときの問題解決のスピードが非常に速く、数分のレベルである。もしインシデント対応をよく理解していない人間が担当した場合は、軽く半日はかかる可能性もある。その間組織は脅威にさらされ続け、担当者は本来行うべき仕事が遅延するということになる。組織の安全を守り、効率を維持できている。
3. 従業員のITスキル向上につながる：Falcon Completeチームの対応から多くを学んでおり、今では何か発生したとき、学んだことを応用できるようになっている。初動、次に何をすべきか、行動とその記録をすべて時系列で残すなど、非常に成長を感じている。
4. 海外拠点も含めて対応を任せられる：数が多くないとはいえ、保護すべき対象である。地理的、時間的問題で置き去りにせず運用に含んでもらえる。

「セキュリティ脅威はビジネスの機会損失に直結します。エンドポイント保護は、製品のみならず運用体制まで視野にしっかり入れ、包括的に考えた方がいい。」と木戸氏。まさにその信念が、バリュエンスグループにおけるFalcon Complete導入という形で実を結んだ。

バリュエンステクノロジーズ株式会社
執行役員CIO コーポレートIT部 部長
コーポレートエンジニア
木戸 啓太 氏

POINT

- 未知のマルウェア検知機能等を評価しFalconプラットフォームを選択
- EDRを運用する上では何より専門性が重要とベンダー提供MDRを選択
- セキュリティエンジニアの雇用人件費問題もクリアーし、鉄壁の守りを実現
- 社内エンジニアもスペシャリストからのナレッジを得られる

CROWDSTRIKE

we stop breaches

クラウドストライク合同会社
お問い合わせ: **http://crowdstrike.jp/contact-us/**