CrowdStrike 導入事例

CROWDSTRIKE

株式会社 バンダイナムコホールディングス様

日本を代表するエンターテインメント企業に安心を提供する「CrowdStrike Falcon Prevent」
AI ／機械学習ベースのマルウェア防御機能と容易な拡張を評価

シグネチャ型アンチウイルス製品による脅威のすり抜けと膨大な量のアラート対応が課題に

バンダイナムコビジネスアークは、玩具やゲームなどの多彩なエンターテイメント分野でグローバルにビジネスを展開するバンダイナムコグループにおいて、管理本部機能およびグループ企業を対象としたシェアードサービスを提供している企業だ。同社の情報システム部の役割は、国内のグループ企業22社（従業員約8500名）を対象に、IT戦略、ガバナンスの立案と推進のほか、システムの開発・運用・保守・セキュリティ対策まで多岐にわたる。

同グループでは、以前よりエンドポイントのセキュリティ対策として、シグネチャ型アンチウイルス（AV）製品を利用していたが、2014年ごろからその機能に限界を感じるようになっていた。

「未知のマルウェアやファイルレス攻撃が急増するなか、AV製品は亜種のマルウェアですら検知できない状況になりつつありました。また、既存AV製品は膨大な量のアラートを上げるため、それらへの対応が追いつかず、結果としてアラートに対し何もできない状況に陥っていました」（中村氏）

日本を代表するエンターテインメント企業としては、個人情報をはじめとする機密情報の漏えいは絶対に許されない。そこで同社はエンドポイントにおけるセキュリティ対策の拡充を行うべく、ベンダー各社から提案を募ったものの、その多くは導入のハードルが高く、費用対効果が見込めなかったため、AV製品を常に最新状態に保ちつつ、OSへセキュリティパッチを当てることで対処していたという。

スモールスタートからの機能拡張が可能 レベル分けにより対応を優先すべきイベントが明確化

しかし、サイバー攻撃は日を追うごとに高度化、悪質化する一方である。このままではグループが危機にさらされると危惧したバンダイナムコビジネスアークでは、抜本的な対策を行うことを決め、2018年の年初より検討を開始した。具体的には、エンドポイント対策を6製品ピックアップして比較。3製品に絞り込み、そこからさらに3カ月ほどかけて評価を実施した。情報システム部 ITインフラ戦略セクション IT環境戦略チームの吉村和氏は「要件としたのは、未知・既知のマルウェア、ランサムウェア、ファイルレス攻撃にしっかり対応できることです。

CrowdStrikeは、AI ／機械学習ベースのマルウェア検知・ブロック機能や、各プロセスの相関、関連性から悪質な振る舞いをブロックする機能を備えた『Falcon Prevent（次世代アンチウイルス）』のみを購入することでスモールスタートでき、必要に応じて『Falcon Insight（EDR）』 や『Falcon Overwatch（脅威ハンティングサービス）』など段階的に機能拡張していくことが可能でした。」と語り、さらに、CrowdStrikeと他製品の違いについても「『Falcon Prevent』だけでもプロセスツリーから侵入経路を追う事ができ、また、関連する各プロセスの挙動（外部通信やファイルの書き込み

導入製品

CrowdStrike Falcon Prevent
NGAV

株式会社 バンダイナムコホールディングス

所在地：東京都港区芝5-37-8

導入時期：2018年6月

URL：https://www.bandainamco.co.jp

2005年9月設立。バンダイナムコグループとして、全世界に100社以上を展開している。商品やサービスを通じ「夢・遊び・感動」を提供することをミッションとし、ビジョンである「世界で最も期待されるエンターテインメント企業グループ」となることを目指す。2018年4月からは中期ビジョン「CHANGE for the NEXT挑戦・成長・進化」を掲げた3ヵ年の中期計画を推進している。

BANDAI NAMCO

等の情報）も簡単に把握する事ができます。他製品もEDR機能を付ければ同様の情報を確認することは可能ですが、AVとEDRのセットでの購入が必須となるためライセンス価格が予算に合いませんでした」と説明する。

「運用面の変化として、これまではAV製品で検知した検体をベンダーに送って分析してもらわないと何が起こったのかわからず、それだけ対応も遅れていました。また、アラートが月に数百件も上がるため、どのアラートから対応すべきなのかがわかりにくかったのです。その点、Falcon Preventは Critical、High、Mediumなど5段階にレベル分けしてアラートを上げてくれるので、優先して対応すべきアラートが明確化されるのがありがたいですね」（中村氏）

これらの特長を評価し、同社は2018年6月にFalcon Preventの採用を決めた。

導入後も誤検知やパフォーマンス影響などはなし 脅威の可視化により大きな安心感が得られた

バンダイナムコビジネスアークでは、2018年7月より事業ユニット単位でFalcon Preventの導入を開始した。まずは同社を含む関連企業からテストを兼ねて導入をスタートし、アミューズメント施設系、トイ・ホビー系へと展開を進めている。

「現在はゲーム開発会社への導入を進めている最中です。開発の現場では特殊なツールを使用したり、特殊な操作を行ったりしますし、開発者はシステム環境の変更に対して敏感なので反発されることも心配していましたが、誤検知やパフォーマンス悪化などは全くなく、スムーズに展開を進めております」（中村氏）

Falcon Preventの導入は、初めは検知モードで既存AVと共存して稼動させ、その後、ブロックモードへと移行し完了した段階で既存AV製品を外すという手順をとっている。共存させている期間において、既存AV製品が検知できなかったマルウェアをFalcon Preventが検知した例もあり、非常に導入効果を感じている。Falcon Preventの運用を開始した後は、これまでのところCriticalは1件もなく、Highが月に1、2件、Mediumが10件程度のアラートで収まっているそうだ。

「何よりの効果は、脅威が可視化され大きな安心感が得られたことですね。優先度の高いイベントにはすぐに対応することができますし、経営層に対しても現状がどうなっているか明確に説明できるようになりました。今後は、定期的にレポートを提出することも検討しています」（中村氏）

また、Falcon Preventはクラウドサービスのため、従来オンプレミスで運用していた既存AV製品のサーバーが不要となり、そのメンテナンス管理にかかっていたコストと労力が大幅に削減されたという。

残りのクライアント、サーバーへの展開を進める

バンダイナムコビジネスアークではさらにFalcon Preventの導入を進め、対象となる1万台のクライアントへの対応後、サーバーへも展開する予定だ。

最後に中村氏は今後について、「経営層からは当グループが常に狙われ、侵入されていることを前提に対策を行うよう言われています。完全な防御が不可能である以上、万が一の際にどれだけ迅速に対応できるかがカギになるでしょう。」と語ってくれた。

POINT

- 未知・既知のマルウェア、ランサムウェア、ファイルレス攻撃への対応を実現
- アラートがレベル分けされているため、優先して対応すべきイベントが明確に
- 初期投資を抑え、段階的に機能を拡張していくことが可能

株式会社バンダイナムコビジネスアーク
情報システム部
ITインフラ戦略セクション
IT環境戦略チーム
アシスタントマネージャー
中村 賢太朗 氏

株式会社バンダイナムコビジネスアーク
情報システム部
ITインフラ戦略セクション
IT環境戦略チーム
吉村 和 氏

株式会社バンダイナムコビジネスアーク
情報システム部
ITインフラ戦略セクション
IT環境戦略チーム
大場 牧夫 氏

CrowdStrike Japan 株式会社
〒104-0031 東京都中央区京橋2丁目2-1 | crowdstrike.jp