CrowdStrike 導入事例

CROWDSTRIKE

株式会社ディー・エヌ・エー様

Falcon Insight（EDR）の誤検知率の低さと運用のしやすさが
SOCの運用負担を大幅に軽減し迅速な状況の把握と対応が可能に

最新の脅威へ対抗するためには既存の対策では不十分

ゲーム、ショッピング、オークション、SNS、決済などのインターネットサービスのほか、スポーツ、オートモーティブ、ヘルスケア等、幅広い領域でビジネスを展開しているDeNA。2011年にはプロ野球に参入し、横浜DeNAベイスターズの観客動員数を7年間で2倍近く伸ばすなど、先見性のある攻めの経営姿勢は常に世の注目を集めている。

これまで同社は、多くのユーザーを抱える企業の責任として、シグネチャベースのアンチウイルス製品をはじめ、脆弱性管理、WAF、資産管理ツール、ログ保存などのセキュリティ対策を導入してきた。しかし、同社が外部機関に依頼してペネトレーションテスト（侵入テスト）を実施したところ、ある程度の被害拡大を許してしまったという。

システム本部 セキュリティ部の松本隆氏は「当社としてもできる限りの対策をとってきた自負はありましたが、この結果を見るに、昨今ますます高度化・巧妙化する脅威に対抗するためには従来のアンチウイルス製品では不十分と判断しました。そこで、隠れた脅威を迅速に検出・隔離し、自社を守る対策としてEDRが必要と考えたのです」と当時を振り返る。また、企業のレピュテーションを高める観点からも、情報漏洩、個人情報保護などに対して、さらにセキュリティ投資を積極的に実施する方針が打ち出された。

それに後押しされ、セキュリティ向上の一環として、SOCの設立と優先順位が高いEDRを導入することが決まった。

業務を妨げない誤検知率の低さと運用面のしやすさを評価し採用決定

DeNAではEDRの導入に際し、5つの製品をピックアップして比較。この際、製品仕様や机上での機能比較、また同社の社内にある端末の半分をMacが占めていることから、WindowsとMac、およびLinuxへの対応を必須とした。

同社は候補をCrowdStrike社の「CrowdStrike Falcon Insight」を含む2製品に絞り込み、2018年6月より1カ月かけて検証を実施。

経営企画本部 企画統括部 IT戦略部システム開発グループの赤坂宇哉氏は「誤検知がどれぐらい発生するのかを重点的にチェックしました。というのも、当社の開発部門は業務における端末の使用についてかなりの権限が与えられており、さまざまなツールの使用が許可されています。そのため、通常とは異なる動作が多く、その正常な挙動が怪しいと判断されて、誤検知が暴発することを恐れていました。

この点、CrowdStrike Falconは当社特有の開発系のツールでも誤検知が極めて少なく、検知精度の高さを感じました。もうひとつの製品は誤検知により、開発系のツールを止めてしまい、対象ユーザーの方に迷惑をかけることが多々ありました」と語る。同社の選定のもう一つのポイントは運用のしやすさ、具体的には直感的に把握できること、全体として何が起きているか俯瞰して見られることにあった。

導入製品

CloudStrike Falcon Insight
EDR

CloudStrike Falcon OverWatch
驚異のハンティング

CloudStrike Falcon Prevent
NGAV

CloudStrike Falcon Discover
IT資産管理

株式会社ディー・エヌ・エー

所在地：東京都渋谷区渋谷2-21-1

導入時期：2018年11月

URL：https://dena.com/jp/

1999年の設立以来、モバイルを中心にゲーム、ショッピング、オークションなど、さまざまなインターネットサービスを提供してきた。2012年からは「Delight and Impact the World（世界に喜びと驚きを）」をミッションに掲げ、スポーツ、オートモーティブ、ヘルスケアなど、インターネット以外の新たな分野に挑戦。各事業へのAI技術の研究・開発・導入にも取り組んでいる。

DeNA

「実際にSOCオペレータに触ってもらったのですが、CrowdStrike Falcon Insightは直感的に全体の状況を把握でき、横断的且つ容易にイベント検索ができる点が好評でした。一方、もうひとつの製品は全体としてのインシデントのつながりが容易に見えなかったのです。これらの点を考慮し、CrowdStrike Falconが当社の目指す運用に合っていると考えました」（松本氏）

同社は、2018年8月にCrowdStrike Falconの採用を決定。9～11月にかけて資産管理ツールを使ってリモートで導入作業を実施し、100台、200台、400台と問題がないことを確認しつつ段階的に展開していった。「導入によって動作が重くならないか心配していましたが、そういった懸念は一切ありませんでした」（赤坂氏）

SOCの運用負荷を大幅に軽減 状況の把握も容易に

DeNAがCrowdStrike Falconを導入した効果として、まず挙げられるのがSOCの運用負荷が大幅に軽減されたことだという。この点についてシステム本部 セキュリティ部 セキュリティ技術グループの星本英史氏は「例えば、オペレータはセキュリティアラートをきっかけに対処を開始しますが、アンチウイルス製品が上げるアラート情報からでは、詳細に調査すべきアラートを絞り込む作業が大変でした。

この点、CrowdStrike Falconはその中でもCritical／High／Mediumなど脅威をランク付けしてくれるので、優先すべき対象が明確になります。

当社では基本的にMedium以上をチェックするようにしており、CriticalとHighについてはリアルタイムで対処することができています」と説明する。また、かつては端末内で動いているプロセスや、どのプロセスから通信が発生したのかなどがわからないという課題があったが、これも解消することができた。

「これまではある程度あたりをつけてログの検索やフォレンジックを実施していましたが、断片的な情報でしか分からず、解析に相当な時間を要していました。今では端末内部が可視化されて、すぐに状況を把握できるようになりました」（松本氏）

さらに同社が便利な機能として評価しているのが、リモートによるリアルタイムレスポンスの機能の実装である。ファイル消去やプロセスの停止、PowerShellの活用など、感染した端末に対してリモートで修復などの対応が可能になったことで、拠点が離れている場合でも迅速に対応できるようになった。

なお同社は今回の導入にあたって、資産管理が可能なオプション「Falcon Discover」も採用している。資産管理ツールは別製品で導入していたが、オペレータにはアクセス権限がなく、EDRとの連携がしづらいという問題があった。しかし、「Falcon Discover」は同じ管理コンソール上でアセット情報を確認できるため、容易にアプリケーションのバージョンなどが即座に把握できるようになり、脆弱性などのリスクにもいち早い対応が可能になった。

POINT

- **それぞれの脅威がランク付けされていることで、優先すべき対象が明確化**
- **調査を実施する際、迅速に一連の流れを把握できる**
- **感染した端末に対し、リモートで修復や隔離などの対処を容易に行える**

システム本部 セキュリティ部
セキュリティ技術グループ
星本 英史 氏

経営企画本部 企画統括部 IT戦略部
システム開発グループ
赤坂 宇哉 氏

システム本部 セキュリティ部
松本 隆 氏

システム本部 セキュリティ部
セキュリティ技術グループ
安永 貴之 氏

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