CrowdStrike 導入事例

CROWDSTRIKE

クックパッド株式会社 様

月間のべ5400万人が利用する人気レシピサービス運営会社を
「CrowdStrike Falcon」がセキュリティ面から支える

オーバーヘッドの解消を目指しNGAV製品を導入するも大量の誤検知が発生してしまう

クックパッドは1997年設立。料理レシピ投稿・検索サービス「クックパッド」の企画・運営、および関連事業を広く展開している。これまで同サービスに投稿されたレシピ数は約300万品、月間のべ5400万人が利用しており、有料のプレミアムサービスの会員も200万人を突破。

また、2014年からは海外への進出を開始し、すでに欧米、アジア、中東などの地域においてサービスイン。26言語、71ヵ国（日本含む）でその地域に根ざしたレシピを提供しており、こちらの利用者数も月間のべ4000万人まで増加している。

同社のサービスを支えるインフラの運用・管理を担っているのが同社の技術部だ。その中のセキュリティグループは、セキュリティシステムの設計・実装、サービスの脆弱性についての診断などを担当しているが、これまでにいくつもの課題に直面してきたという。技術部セキュリティグループの三戸健一氏は「非常に多くのユーザに利用していただいている以上、当社のサービスにとってセキュリティの担保は最も重要な課題のひとつです」と説明する。

エンドポイントセキュリティについて、「以前はシグネチャベースのアンチウイルスソフトを導入していたのですが、次第にオーバーヘッドが増大し、業務に支障をきたすようになっていました。例えば、開発環境でソースコードの全文検索をローカルPCで実行すると、何分も待たされて作業の効率が大幅に低下していたのです。そこで、2015年の夏、機械学習を採用したNGAV製品に切り替えたという経緯があります」と過去を振り返る。

この導入によりオーバーヘッドの問題は解消できたのだが、今度は誤検知という別の問題が発生してしまった。例えば、今までになかったようなバイナリーファイルが入ってくると大量のアラートが発生する。メモリー監視を機能させるとデータベースのプログラムが起動できなくなる…といった具合である。

そのため、ポリシーをゆるく設定しないと運用ができない状態だった。技術部セキュリティグループ グループ長の水谷正慶氏は「最大の問題は、開発環境において誤検知が多発したことです。

しかも、アラートに含まれている情報の量が少ないため、インシデントについて追跡調査ができず、途中でクローズせざるを得ないこともたびたびでした」と当時の状況を語る。

また、当時の同社では、管理には製品のコンソールをそのまま利用しており、APIでの製品間連携や、様々なログの取得、長期保存などは整っていなかった。しかし近年、脅威がますます高度化していく中、イベントの検知・ブロックだけでは十分といえなくなってきたのである。

「そこで、端末上のアクティビティを監視し外部との通信などを追跡できるようにするしくみが必要と考えました」（水谷氏）

データを確実に取得でき既存システムとも連携可能なCROWDSTRIKE FALCON

こうした課題を解決するため、クックパッドは2018年5月よりEDR製品の導入を検討。「今回の導入の要件としては、社外からのアクセスも含め私たちが必要とするデータを確実に取得できること、セキュリティ監視装置など既存システムとの連携がとれること、などがありました。他製品の場合、単体では対応が難しくインシデントレスポンスツールなどと併用する必要があったり、業務用の開発環境をセットアップすることがスムーズに行えなかったりという問題が存在していましたが、CrowdStrike

導入製品

CrowdStrike Falcon Insight
EDR

CrowdStrike Falcon Prevent
NGAV

CrowdStrike Falcon OverWatch
驚異のハンティング

クックパッド株式会社

所在地：東京都渋谷区恵比寿4-20-3

導入時期：2018年8月

URL：https://cookpad.com/

“毎日の料理を楽しみにする”というミッションのもと、料理レシピ投稿・検索サービス「クックパッド」の企画・運営を中心にビジネスを展開。現在その利用者数は月間のべ5,400万人を超えており、英国やスペイン、インドネシアなど海外への進出も積極的に進めている。2009年には東証マザーズに上場、2011年には東証一部に上場した。

cookpad

社製品に関してはそうした問題はありませんでした」（三戸氏）

同社はCrowdStrike社製品のPoCを実施した後、社内の各部署のエンジニアの協力を得て、実際の開発環境にもテスト導入した。

CrowdStrike Falconは一つのエージェントで多数の機能を利用できる。同社はEDR（Falcon Insight）と脅威ハンティングサービス（Falcon OverWatch）のみの導入を検討していたが、NGAV（Falcon Prevent）も検証の中で機能を確認することができた。

「当社はmac OSが基本で、全体の8割を占めている環境なのですが、問題なく導入できました。また当初は、EDRと脅威ハンティングサービスのみの導入、API連携で社内システムとの統合を検討していました。

しかし既存で導入していたNGAV製品をFalcon Preventに置き換えることが可能とPoCで判断することができたため、同時採用へと至りました。従来の課題であった開発環境における誤検知は激減しましたし、クライアントへの負荷が少なく、作業に影響を与えないのもよかったですね」（水谷氏）

通信イベントの詳細な把握が実現出張やリモートワークなど社外からのアクセスにも対応

同社は、Falcon Insightを導入したことで、通信イベントを詳細に把握できるようになり、調査の深掘りが可能になった。

「たとえばゲートウェイで怪しい宛先への通信を検知した際、これまでは担当者に対して何をしていたか聞きに行くしかありませんでした。しかし、Falcon Insightを導入したことで、ログからクライアントの中で何が起きているのか動きがわかるようになり、担当者にヒアリングを行わずとも、調査や判別を行うことができるようになりました。

また、システム連携により自社環境にログを転送して長期保存できるようになり、経路の追跡はもちろん、外部とのアクセスの有無などを含めて辿ることが可能になっています。時系列での把握、プロセスの一連の動きも確認できるのは大きいですね。画面もグラフィカルで状況が一目瞭然です」（三戸氏）

また、情報量が増えたことで、対応の選択肢も増えたという。誤検知とそうでないものとの差も明確に判断できるようになった。

「以前は本来ブロックすべきでない通信を止めてしまったこともありました。しかし、CrowdStrike Falconの導入後は、ユーザからセキュリティソフトによるPC不具合等の問い合わせは全くなくなりました」（水谷氏）

出張やリモートワークなど、社外からのアクセスへ対応できる点も評価している。

「当社では部署ごとの判断でリモートワークを認めていますが、社外にいる端末に関しても追跡調査が可能なので、安心して利用を認めることができます」（水谷氏）

また同社では、EDRのログと既存のログ管理システムとの連携も重視しており、CrowdStrike FalconがAPIやAWSのS3やSQSを利用したDataReplicatorといったログ転送の仕組みを利用し、自社のログ管理システムと統合し活用している。検証段階より、これらの機能を利用してログ転送を検証した結果、CrowdStrike Falconの用意している機能が充実しており、有効であることを判断した。

「Syslogでログを転送するサービスの場合ですと、途中でログが欠損してしまった場合など運用負荷の課題がありました。その点、CrowdStrike FalconのDataReplicatorログ転送の仕組みは画期的でした。現在はCrowdStrike Falconから発生したアラート情報や、プロセスの動きや通信の動きなどの通常のイベントを自社のログ管理システムに連携し運用しています」（水谷氏）

それだけではなく、CrowdStrike Falconにはマネージドで提供される脅威ハンティングサービス「Falcon OverWatch」があり、24時間365日体制で攻撃の兆候となる挙動を検知、調査している。

「われわれが発見することが困難な挙動も確実に検出してくれるという意味では非常に安心感がありますね」（三戸氏）

海外への展開についても検討処理の自動化やSSO連携も視野に

技術部セキュリティグループ
グループ長
水谷 正慶 氏

技術部セキュリティグループ
三戸 健一 氏

クックパッドでは、国内におけるCrowdStrike Falconの導入が完了したことから、次なる段階として海外への展開を検討している。また、一定の条件を満たした場合は誤検知に分類するなど、処理の自動化を目指すとともに、シングルサインオン（SSO）連携も進めていくという。

POINT

- EDRとNGAVを1つのエージェントで実現
- 通信イベントを詳細に把握し、社内システムと連携することで確実な追跡調査が可能に
- 出張やリモートワークなど、社外の端末監視にも対応

クラウドストライク 株式会社
〒104-0031 東京都中央区京橋2丁目2-1 | crowdstrike.jp