Fal.Con 2021: Falcon XDRとCrowdXDR Allianceの紹介

October 12, 2021 | George Kurtz | Endpoint & Cloud Security | Executive Viewpoint

これは、10月12日～14日に開催の「CrowdStrike主催サイバーセキュリティイベント Fal.Con 2021」の発表内容の一部です。

CrowdStrikeの私たちのミッションは、今日も2011年と同じです。つまり、「stop breaches」侵害を阻止することです。

私たちの使命を達成するためには、攻撃を即座に阻止するだけでなく、サイバーセキュリティの将来のニーズと巧妙化する攻撃者グループの戦術の先手を打つために特別に構築されたプラットフォームが必要になることを私たちは理解しています。今日のFal.Con2021で、CrowdStrikeは再びセキュリティの業界標準を定義し、現在の高度な攻撃を阻止するための最も強力な武器をお客様に提供することで、皆様が直面している課題に対応できるよう支援致します。

Falcon XDRの紹介、そして**CrowdXDR Alliance**

これらの発表と、それらがお客様にとって何を意味するのか、私は非常に興奮しています。 **Falcon XDR**は、業界をリードするEDR（エンドポイントでの検知と対応）をエンドポイントを超えて拡張し、業界の他のどの製品よりもはるかに優れた可視性、リアルタイムの脅威検知、および自動応答をお客様に提供します。

また、XDRがセキュリティの歴史の中で単なる流行語にならないように、業界のリーダーとの画期的な新しいアライアンスである**CrowdXDR Alliance**は、企業全体のセキュリティに対する最高のプラットフォームアプローチをお客様に提供します。

しかし、これらのエキサイティングな両方の発表に入る前に、一歩下がってXDRとは何かを正確に定義したいと思います。セキュリティ業界の多くのものと同様に、XDRは、ベンダーの主張に駆り立てられて多くの誤解を招き、混乱を引き起こしています。

誇大広告とは一線を画す現実解: XDR Edition

セキュリティチーム、リーダーは、あらゆる場所で**"XDR" — extended detection and response**（拡張された検知と対応）という用語を目にしています。

SIEMベンダーは、関連性を維持しようと努力し、この用語を利用しています。レガシーなエンドポイント、いわゆる次世代と言っているエンドポイント、これらのプレーヤー達は、弱点を隠すために、古いプラットフォームをXDRとして再パッケージ化することにしました。

また、流行語に飛びついているのは、ファイアウォールならびにネットワークベンダーであり、多くのベンダーが、単に顧客をさらに閉じ込める方法として「ネイティブ」XDR機能を主張しています。独自のテクノロジーを統合する理由は、顧客を幸せにすることではなく、この市場に参入するために最低限必要な条件だからです。

問題は、これらの主張にもかかわらず、ベンダーの多くが行っていることは、セキュリティチームにさらに多くのデータと複雑さをあふれさせることによって、セキュリティ問題を悪化させているだけであるということです。過去と同じ失敗したアプローチを取ることは、今日の攻撃者グループからお客様を助けることにはつながりません。

簡単に言うと、概念としてのXDRは、企業全体から実用的なインサイトを導き出し、脅威が存在する場所を阻止することで、お客様のセキュリティスタックの混沌とした配列に秩序を適用することを目的としています。

XDRは**EDR**テクノロジーから始めて、そこから構築する必要があります。EDRの拡張であり、セキュリティスタック全体からの最

も関連性の高いテレメトリでEDRデータを強化する必要があります。複数のテクノロジーやドメインにわたって、リアルタイムの脅威検知、アラート、ハンティングを提供する必要があります。そして最後に、XDRは、セキュリティスタック全体にわたる脅威アクティビティへのプロアクティブな自動対応を提供する必要があります。

Falcon XDR: エンドポイントを超えた保護

これはまさに**Falcon XDR**がお客様に提供するものであり、セキュリティデータを理解し、脅威が存在する場所を見つけて阻止するためのより良い方法です。**CrowdStrikeFalcon®プラットフォームは、この瞬間のために構築されました**—セキュリティデータの力を利用し、お客様が攻撃者グループの戦術の変化に先んじた対策を打てるようにします。

これが、Humioの買収と、そのテクノロジーをFalconプラットフォームへ統合すること、XDRの分水嶺の瞬間を表す理由でもあります。

Humioを基本的なアーキテクチャコンポーネントとして使用することで、Falcon XDRは、ネットワークセキュリティ、電子メールセキュリティ、クラウドのIaaSとPaaS、SaaS、CASBなどからのデータをCrowdStrikeセキュリティクラウドにおけるCrowdStrikeの業界をリードする脅威インテリジェンスと相関させます。Falcon XDRは、CrowdStrikeが世界規模で活用している機械学習、人工知能（AI）、攻撃の指標（IOA）をこのデータに適用して、セキュリティスタック全体にEDRの結果と高度な脅威検知を拡張し、侵害をより迅速に阻止します。

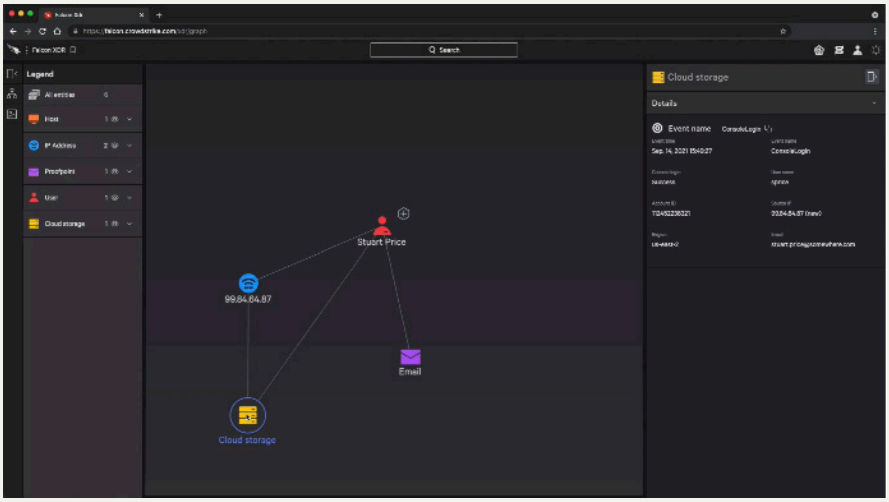
これにより、XDRのビッグデータの課題が解決され、誤検知、アラートの疲労、および膨大なデータ処理とストレージのコストが排除されます。

しかし、それだけではありません。セキュリティワークフロー全体で対応を調整および自動化するためにFalconプラットフォームにネイティブに組み込んだ、CrowdStrikeの**SOAR framework**である**Falcon Fusion**がすべてのお客様に無料で提供されることも発表しました。

FusionはXDRのRを担います。お客様は、検知とインシデントの分類に基づいてカスタマイズ可能なトリガー設定を利用し、リアルタイムのアクティブな通知および対応機能を構築できます。これにより、運用シナリオの要件を満たしながら、SOCとITの効率と俊敏性が向上します。

これがFalconXDRを際立たせ、CrowdStrikeがセキュリティとITスタック全体にわたって真の組織全体に渡る脅威の検知、調査、対応、およびハンティングを提供することにより、XDRのビジョンを実現できるようにするものです。

こちらのデモで実際に動作しているFalconXDRをご覧ください：



CrowdXDR Alliance: 画期的なアライアンス

CrowdXDR Allianceの設立時からのパートナーであるGoogleCloud、Okta、ServiceNow、Zscaler、Netskope、Proofpoint、Extrahop、Mimecast、Claroty、Corelightの皆様が、XDRがお客様に価値を提供できるように協力してくれたことに感謝します。

組織はこれ以上のセキュリティアラートを必要としません。複雑な攻撃を阻止するには、セキュリティスタック全体で最も関連性の高いインサイトが必要です。ただし、セキュリティプラットフォーム間でのデータ共有に関する従来の標準の欠如により、調査と脅威ハンティングにギャップが生じています。

CrowdXDR Allianceは、セキュリティツールとプロセス間でデータを共有するためXDRにおける共通の言語を確立し、最も関連性の

高いベンダー固有のセキュリティテレメトリによりEDRデータを強化することで、これらすべての課題を解消していきます。 この画期的な進歩により、すべてのドメインでリアルタイムの検知と脅威ハンティングを可能にする統合XDRソリューションがお客様に提供されます。

比類のないセキュリティ効率と有効性を提供することにより、お客様の全体的なセキュリティエクスペリエンスを向上させるために、これらのパートナーが参加してくださることを非常に誇りに思っています。

Fal.Con 2021: ご自身で体験ください！

FalconXDRとCrowdXDRAllianceの詳細についての、重要なセッションをいくつか紹介します：

- **Fal.Con 2021 基調講演：The Power of We**
- **XDR：何がXDRで、何がXDRでは無いのか。XDRのあるべき姿について！**

こちらのサイトよりご覧いただけます。

これらは、Fal.Con 2021で行ったエキサイティングな発表のほんの一部です。XDR以外にも興味深い発表、セッションが行われました。チェックする機会がなかった場合は、ぜひこれからチェックしてみてください。 それらすべてを今後数か月間で利用できるようにします。

Fal.Conは、組織が直面する最大のセキュリティ課題を解決するために私たち全員が集まるべき場所です。お客様のセキュリティ対策の効果を改善するには、統一されたアプローチが必要です。 これがCrowdStrikeが構築しているものです。これは、『Stop Breaches ～侵害を阻止する』という共通の目標を共有する強力なコミュニティでもあります。

参考情報

- Falcon XDR と CrowdXDR Allianceについてご紹介しています（英語）。
- Falcon XDR Demo（英語）をご覧ください。
- Falcon Fusionの詳細を webpage や blog でご覧ください（英語）。
- CrowdStrike Falcon プラットフォームのページで組織、従業員、およびデータがどこにあってもそれらを包括的に保護する方法をご覧ください。
- CrowdStrike Falcon Prevent™のフル機能を無料でお試しいただき、今日の最も巧妙な脅威に対する真の次世代AVの性能をご確認ください。

原文：Fal.Con 2021: Introducing Falcon XDR and CrowdXDR Alliance
https://www.crowdstrike.com/blog/introducing-falcon-xdr-and-crowdxdr-alliance/