CrowdStrikeの統合SOARフレームワーク、Falcon FusionでSOCを最新化

12 October 2021 | Amol Kulkarni | 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。

セキュリティオペレーションセンター（SOC）ではセキュリティの専門家が2つの大きな戦いに悩まされています。1つ目は、高度な技術を駆使して防御を突破しようとする、巧妙化した攻撃者に対する戦い、そして2つ目は、この1つ目の攻撃に勝つために必要な、増え続ける複雑なセキュリティスタックに対する戦いです。

侵入を阻止し、攻撃者との戦いに勝つためには、1秒たりとも無駄にすることはできません。セキュリティにおいて断固たる対応が必要な状況では、スピードと効率が求められます。しかし、人員が不足しているセキュリティチームは、システム間でさまざまなデータを生成する複数のポイントソリューションを管理しなければならないことに悪戦苦闘しています。

私が話を聞いたセキュリティの専門家は、一様に同じことを言います。「今日の攻撃者との戦いに勝つためには、迅速さ、簡単さ、そして自動化が必要である」と。スピードと効率を向上させるには、セキュリティプラットフォームに組み込まれた自動化が必要となり、また、社内プロセスに合わせたカスタムのワークフローも作成しなければなりません。

CrowdStrikeの目標は、セキュリティチームが今日のサイバー戦争に勝利し、将来に備えるために必要な技術とサポートを提供することです。そのため、本日開催されたFal.Con 2021では、クラウドSOAR（Security Orchestration Automation and Response）フレームワークである**Falcon Fusion**を、Falcon Prevent™とFalcon Insight™を使用するすべてのCrowdStrikeのお客様に無料で提供することを発表しました。

複雑なワークフローの自動化とオーケストレーション

1-10-60 SOCチャレンジを達成するには、企業のSOCチームは平均で、攻撃を検知するのに1分、それを調査するのに10分、そして封じ込めに1時間で対応する必要があります。セキュリティチームの問題として、セキュリティスタックの相互運用が可能でない点、そして最新のセキュリティソリューションには顧客の実際の問題と目標とする結果に基づいて、ポリシーを直感的にカスタマイズして構築する機能がないことが多い点が挙げられます。

その一方で、バランスを取る必要もあります。カスタマイズ性が高すぎると、複雑で理解しにくいポリシーとなり、実際の目標とする結果から逸脱してしまう可能性があるからです。CrowdStrikeが委託した最近のグローバルITセキュリティ調査（**Supercharge Your Security Transformation: A Two-pronged Approach for IT Security**）では、回答者の71%が、他のテクノロジーやセキュリティスタックとの統合が複雑であるため、組織における改善が必要であるとしています。また、回答者の92%が、組織がセキュリティソリューションに関する運用上の課題を抱えていると答えています。

企業のSOCアナリストに共通する不満としては、さまざまなシステムにまたがる複数の（ 時には重複する）アラートの分析や対応に時間がかかってしまい、その結果、アラート疲れと対応時の効率の低下を招くというものが挙げられます。同調査によると、自組織でアラート疲れが問題になっていると回答した人は80%に上っています。

Falcon Fusionは、複雑で繰り返し発生するタスクのオーケストレーションと自動化を行うことで、**SOCオペレーション**を刷新して生産性を向上させ、SOCチームの大幅な効率化を図ります。

Falcon Fusionは、**CrowdStrike Falcon®プラットフォーム**によって提供される堅牢かつ業界をリードするエンドポイントおよびワークロード保護と統合されています。CrowdStrike Security Cloudの優れた機能を活用して、エンドポイント、アイデンティティ、ワークロード全体で関連するコンテキストインサイトと、パートナーアプリケーションからのテレメトリを組み合わせることで、複雑なワークフローをオーケストレーションして自動化します。企業のお客様は、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とともに、複雑な順序付けや分岐を利用して、リアルタイムのアクティブな通知やレスポンス機能を構築できます。これにより、ユースケースの要件を満たしながら、SOCとITの効率性と俊敏性を向上させることができます。

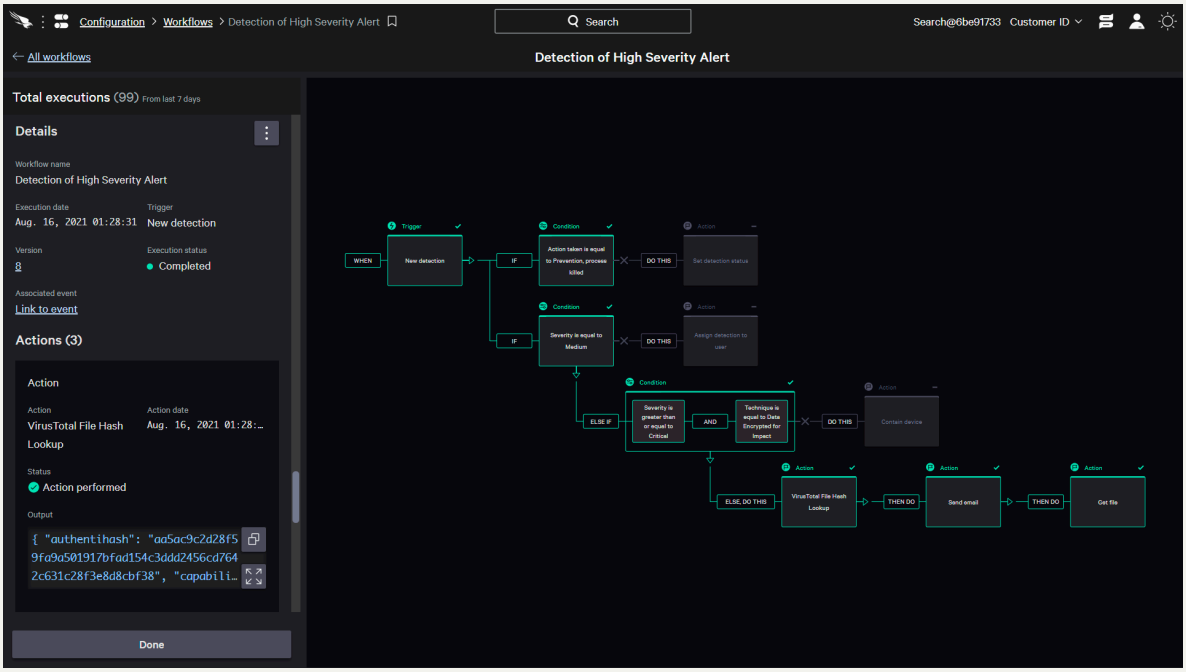
Security Cloudの力

世界最大級のクラウドアーキテクチャを構築したサイバーセキュリティ企業として、CrowdStrikeはこれまでにない可視性とコンテキストをすべて1か所で提供しながら、**インシデント対応**を合理化するために必要な優れた視点を獲得し、独自の経験を積み重ねています。

CrowdStrike Security Cloudは、ストリーミングデータだけでも、1日に1兆件以上のイベントを処理し、毎秒1億4,000万件を超える**IOA（Indicator of Attack）**の判定をしています。さらに、CrowdStrikeがクラウドに保存しているデータは15ペタバイトを超えており、毎日数十億ものエンティティ（ワークロード、エンドポイント、アイデンティティ）を保護しています。これらすべてのデータを、**CrowdStrike Store**を通じてアクセスできるパートナーデータと組み合わせることで、環境全体で発生しているイベントを可視化し、アクティブレスポンス機能を強化して、インシデント対応と修復を効率化できます。

通知の効率化とFalconリアルタイムレスポンス（RTR）ワークフローの高速化

オープンなセキュリティクラウドのエコシステム上に構築されたFusionは、強力なコンテキストインサイトを備えており、お客様はアラート、検知、インシデントをトリガーとして使用し、ノーコードロジックを使って反復可能で一貫性のある自動化を構築できます。また、アナリストは、繰り返し発生する手動タスクを自動化することで多くの時間を節約し、よりビジネスクリティカルな戦略的責任に集中することが可能になります。Falconコンソールの高度なワークフロービルダーを使用すると、ユーザーはトリガーを簡単に可視化し、特定の条件に基づいて自動化アクションの複数の潜在的なルートを作成し、処理が行われたワークフローのパフォーマンスを監視することができます。また、ワークフロービルダーは、条件分岐ロジック（「if」、「else if」、「else」）や、シーケンシャルフローと並列フローの両方をサポートしており、セキュリティチームが有効性と効率性を損なうことなく、組織の要件を満たせるようにします。

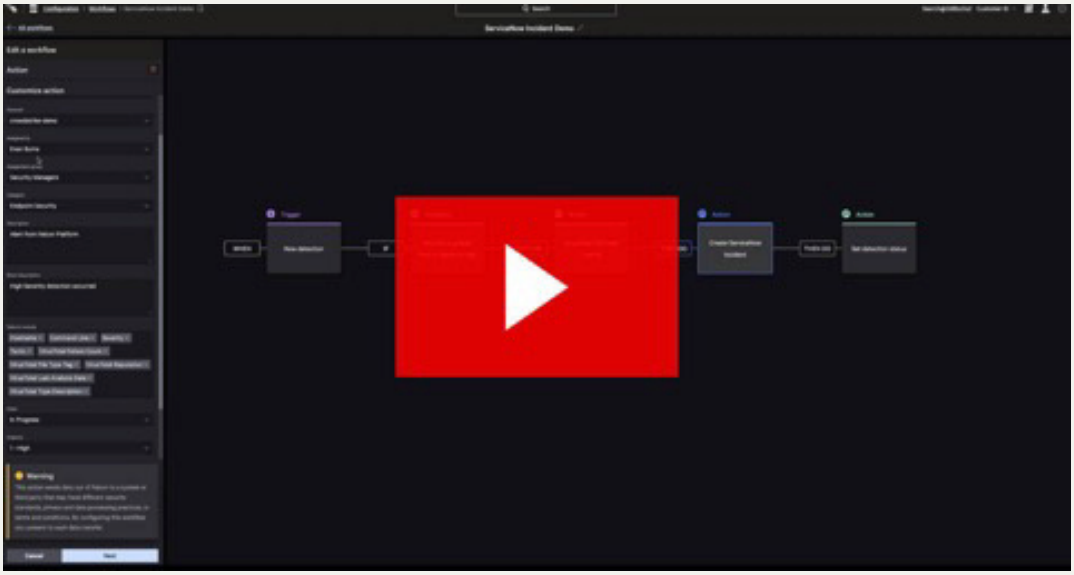


クリックして拡大

ワークフロービルダーは通知プロセスもサポートしているため、アナリストは一連の重要なタスクを反復可能で標準化されたプロセスへと自動化し、選択したコラボレーションチャネル（Slack、PagerDuty、Microsoft Teams、メールなど）全体でカスタマイズされた通知をタイムリーに受け取ることができます。これにより、重要なアラートに集中できるようになります。

通知アクションのサポートに加えて、Fusionワークフローは、脅威の検知、インシデント、監査イベントに基づいて統合コンソールからシームレスに実行できる潜在的なアクションの拡張コレクションをサポートし、Falconプラットフォームおよびサードパーティアプリケーションからもたらされるコンテキストインサイトを提供します。アナリストは、Falconリアルタイムレスポンス

（RTR）機能により、自動化を活用することもできます。また、高度なアクションの自動化とオーケストレーションを行うことも可能です。たとえば、設定した一連のイベントに基づいて侵害されたホストや疑わしいホストを隔離したり、コンテキストを充実させるためにVirusTotalの検索を実行したり、トリアージアクティビティ（ファイルやプロセスの取得、ファイルの削除、プロセスの停止など）を実行したりすることができるため、結果的に脅威を修復するまでの平均時間が短縮されます。



Falcon Fusion がどのように機能するのか、動画でご覧いただけます。

CrowdStrikeのお客様のためのFalcon Fusion

今日の組織は、マルチクラウド環境や地理的に分散している従業員などの拡大する攻撃対象に対処しており、増え続けるアラートを選別してビジネスの安全を確保することがセキュリティチームの大きな負担となっています。Falcon Fusionは、CrowdStrikeのお客様に豊富なコンテキストインサイトと価値の高いカスタマイズを提供して、差し迫ったニーズを満たすだけでなく、反復可能なワークフローを大規模に展開できるように構築されています。Fusionは、CrowdStrikeのSecurity Cloudが提供する包括的な可視性と、軽量なFalconエージェントが提供する強力なインシデント対応機能を組み合わせて、複雑なSOCワークフローの自動化と簡素化を実現します。FalconコンソールからFalcon Fusionにアクセスして、今すぐワークストリームを簡素化する方法をご確認ください。

参考情報

- Falcon Fusionのデモはこちらから（英語）ご覧いただけます。
- Falcon Fusionについて詳しくは、ウェブページ（英語）をご確認ください。
- Falcon Fusionのデータシート（英語）をダウンロードして詳細情報を入手できます。
- 強力なCrowdStrike Falconプラットフォームが、場所を問わずに、組織や従業員、データを包括的に保護する仕組みをご紹介します。
- 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の性能をお確かめください。

原文：Modernize Your SOC with Falcon Fusion, CrowdStrike's Integrated SOAR Framework
https://www.crowdstrike.com/blog/how-to-modernize-your-soc-with-falcon-fusion/