Falcon FileVantage：CrowdStrikeの新しいファイル整合性監視ソリューションでSecOpsの総合的な効率化を実現

October 12, 2021 | Amol Kulkarni | Endpoint & Cloud Security | Executive Viewpoint

本件は、10月12日～14日開催Fal.Con 2021 CrowdStrikeサイバーセキュリティカンファレンスにて発表されました。

組織のベース、マスターであるファイル、フォルダ、レジストリは“クラウンジュエル”と呼ばれ、SecOpsに携わるメンバーはこの”クラウンジュエル”の保護において、しばしばジレンマに直面します。IT部門は多くの資産に対する変更を監視しなければなりません。変更の一つ一つも、その規模が大きくなれば、組織内における監視プロセスは即座に破綻してしまいます。SecOpsは大量のアラートや通知の処理に忙殺されるようになり、それらの変更が発生した資産の周囲で起きている危険なふるまいを見逃してしまうことになりかねません。

様々な規制などは、これらの重要な資産やシステムの変更を監視する事を、多くの組織に求めていますが、SecOpsスタッフが現在利用できるソリューションでは、効率性が欠けていることがあります。仕方なく複雑なソリューションスタックを組み合わせて、ニーズに合ったファイル整合性監視（FIM）ソリューションを構築して運用しょうと試みる企業は多いものの、それでは必要な可視性が得られないばかりか、とてつもなく高価なものになってしまいがちです。

CrowdStrikeの新しいFalcon FileVantageは、単にコンプライアンス要件を満たすだけでなく、このような課題を解決します。CrowdStrike Falcon®プラットフォーム内で提供されるこのFIMソリューションは、一元的な可視性を実現し、ITチームのアラート疲れを軽減して効率性を高めます。他のFIMソリューションとは異なり、CrowdStrikeの脅威インテリジェンスデータから知見が得られるため、ITチームは攻撃者グループの攻撃活動に直結するファイル変更であるかを見極められるようになります。

図1：Falcon FileVantage の直感的なダッシュボードで一元的な可視性と重要な知見を提供

一元的な可視性とSecOpsの効率化を実現

Falcon FileVantageは、組織内のあらゆる重要な資産、ファイル、レジストリ、システムの作成、削除および変更について、包括的な可視性をリアルタイムで提供します。PCIデータセキュリティ基準（PCI DSS）、米国国立標準技術研究所（NIST）、2002年サーベ

ンスオクスリー法（SOX）をはじめとする規制の多くが、重要なデータへの不正なアクセスや変更を監視・防御するためのコントロールを企業に要求しています。組織環境内で発生するすべての有害な変更を適切に可視化することが不可欠です。

Falcon FileVantageの包括的なダッシュボードと便利なチャートでは、組織に関連するすべてのものを視認できます。また、その可視性を合理化して、最も侵害を受けているシステムや、ファイルのプロパティの変更、アカウントレベルやユーザーレベルのふるまいの変化を監視することもできます。

脅威インテリジェンスデータでコンテキスト情報を強化

Falcon FileVantageでは、システム上の変更をリアルタイムで可視化することに加え、インシデントの発生中/発生後の重要なコンテキストも提供され、これを調査に活用することができます。たとえば、万一組織内でランサムウェア攻撃が発生した場合には、お客様のスタッフがFileVantageコンソールを使用して、発生した攻撃に関連するファイル/フォルダの変更を特定し、FIMコンソールから直接脅威を検知することができます。このデータによって、チームは環境内での攻撃者の活動をピンポイントで特定し、影響を受けたファイルの修復作業の優先順位付けを迅速に行えます。Falcon FileVantageは、スタッフが攻撃者の活動に直結するファイル変更データを突き止め、その活動をハッシュに関連付けます。

CrowdStrikeの脅威インテリジェンスは、国家主導の攻撃者やサイバー犯罪者(eCrime)、ハクティビストなどの160以上のプロファイルを追跡しており、セキュリティチームが攻撃者グループや攻撃技術の動向を常に把握できるように画期的な情報を提供しています。より強固なセキュリティ態勢を確立するためには、この脅威インテリジェンスとファイル監視機能が極めて重要な役割を果たします。

Falcon FileVantage FIM でセキュリティの防御力を強化

ついにアラート疲れから解放されるときがきました。Falcon FileVantage は、SecOps にコンプライアンス遵守の用途に留まらない可視性を提供します。リアルタイムの監視機能と脅威インテリジェンスが提供するコンテキスト情報により、資産とシステムの周辺で発生する危険な行動の全容が明らかになります。御社にとって重要なファイルやフォルダを保護するための「防衛の最前線」としてご利用ください。Falcon FileVantage に関する詳細情報については、Fal.Con 2021 セッション「**Falcon によるファイル整合性監視**」と**プレスリリース**をご覧ください。

その他のリソース

- Falcon FileVantageに関するプレスリリース（英語）をご一読ください。
- Fal.Con 2021セッション「Falconによるファイル整合性監視」をご覧ください。
- パワフルでクラウドネイティブなCrowdStrike Falcon®プラットフォーム全体像については、製品のウェブページをご覧ください。

原文：Falcon FileVantage: New CrowdStrike File Integrity Monitoring Solution Creates Total Efficiency for SecOps
https://www.crowdstrike.com/blog/introducing-falcon-filevantage/