FireEye Helix SOAR

セキュリティ・オペレーション、自動化、レポートにより、セキュリティ・リスクを低減

セキュリティ・オペレーションの管理は、すべての組織にとって難しい課題です。セキュリティ・チームは数多くのツールを利用していますが、それでも大量のアラートへの対応に忙殺されています。

手作業での対応に依存する従来のSIEMとは異なり、FireEye Helixは、各種のテクノロジーやインシデント対応プロセスを単一のコンソールに統合することによってセキュリティ・プロセスを連携し、脅威の検知と対応を迅速化し、シンプルにします。セキュリティ・ツールを統合することによって、セキュリティ・タスクのルーチンを自動化し、本当に重要な脅威への対応に集中することができます。

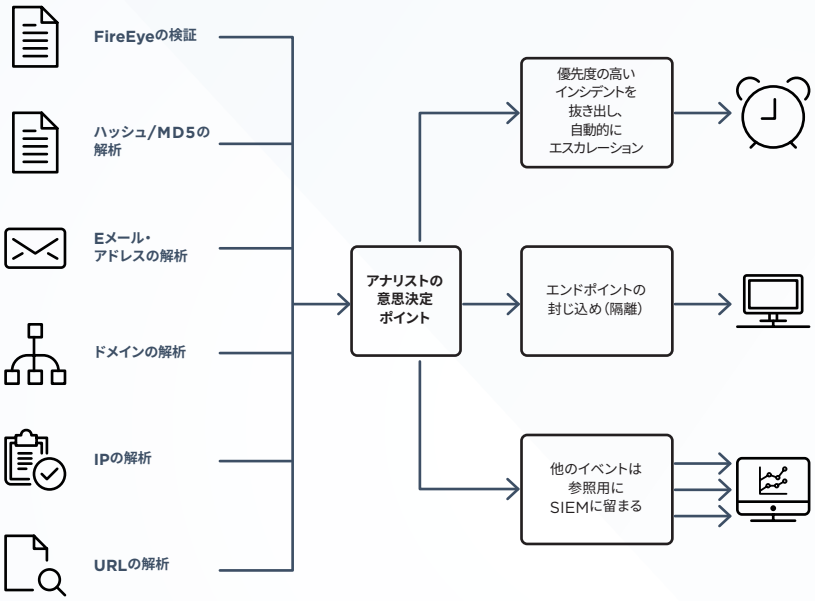

図1: FireEyeのセキュリティ・プロセス連携のしくみ

メリット

- **侵害への対応時間を短縮:** ワークフローの自動化、カスタマイズ可能なダッシュボード、あらかじめ作成されたプレイブックを適用することで、アナリストが優先度の高いタスクに集中でき、リスクを低減
- **既存のセキュリティ投資に対するROIを最大化:** ファイアウォール、アンチウイルス、チケット管理システムに対する何百ものサードパーティ製プラグインを活用し、セキュリティ・オペレーションを管理
- **アナリストに対するワークロードを軽減:** カスタマイズ可能で完全に自動化されたワークフローを導入することで、アナリストの作業量を減らし、プロセスの一貫性を維持

その他の機能

インシデント対応プレイブック

FireEye Mandiantのインシデント対応担当者が開発した、あらかじめ構築された400を超える行動計画を用いて、アナリストのスキルを高め、調査を迅速化します。

オープンなプラグイン・フレームワーク

150を超えるサードパーティ製ツールとデータ・ソースを統合して、セキュリティ対策をシームレスに一元管理します。

プロセスの自動化

セキュリティ製品間で、カスタムのインシデント対応ワークフローの自動化を導入します。

ケース管理

使いやすいケース管理システムに、関連するアラートと痕跡を保存することにより、アナリストとインシデント対応チームの共同作業が可能になります。

ケースの割り当て

役割別のグループを作成し、プレイブックに詳細な権限の割り当てを行い、ワークフローの管理を強化します。

使いやすいユーザー・インターフェイス

セキュリティ・チームは、シンプルな抽象化レイヤーでセキュリティ・ツールに簡単に接続し、情報の取得とプッシュを行うことができます。変更をネットワーク・レベル、ホスト・レベル、アプリケーション・レベルで管理します。

FIREEYE HELIXを入手するには?

FireEye Helixは、単体製品、あるいはFireEyeの各ソリューションをサブスクリプションでご購入いただいたときに、併せて入手いただけます。FireEye製品と連携するほか、サードパーティのセキュリティ製品との統合も可能です。日常のオペレーションに影響を与えることなく、組織の成長や変化に合わせてFireEyeソリューションの設定変更、追加やアップグレードを行うことができます。

FireEye Helixの詳細については、**www.fireeye.jp/solutions/helix**をご覧ください。