McAfee Investigator

エキスパート レベルの分析調査を可能に

McAfee® Investigator は、アナリストが問題の根本原因を自信を持って識別し、より多くの問題をより迅速に解決するのに役立ちます。トリアージ (重要度で優先順位付け) されたアラートが送られると、エキスパートは迅速かつ完全に脅威を検証してそれに対応するために、データ収集やエビデンス解析、洞察を行います。

セキュリティの運用上の課題

巨大なイベント量とデータ保存期間により、アラートの重要度と範囲を正確に評価するのは困難になっています。正式なインシデントとして扱うべきかどうかを決定するためのコンテキストや知識が欠けているために、アナリストはしばしばアラートを無視します。

選択したインシデントの調査においては、問題の核心を探るために長時間かかることがあるうえ、脅威ベクトル全体に関する深い専門知識が必要となります。これらの傾向は、熟練したセキュリティ アナリストの必要性が高まっている一方、利用可能な人材は増えていないことを意味しています。

新しい調査分析

この問題に取り組むためには、セキュリティ オペレーション チームは、アラートのトリアージと調査を迅速化かつ効率化して、既存の要員と新人アナリストがより多くの処理をできるようにしなければなりません。

McAfee Investigator は、セキュリティ オペレーション チームがトリアージ、包括的データ収集、そして高度分析を含む調査を行うためのガイドを提供します。エキスパート システムとエンドポイント キャプチャ ツールは、SaaS サービスとして既存のデータソースおよびセキュリティ管理システムと統合し、最小限の労力で短時間で価値を生み出します。

これらのインタラクティブな分析によって、継続的にアップデートされるガイダンスが提供されるため、インシデント対応者はより短時間でより正確にマルウェア、ネットワーク脅威、攻撃の痕跡 (IoC) を調査できるようになります。

インサイトを迅速に発見

McAfee Investigator は、すぐに注意を引けるようにセキュリティ操作が特定の状況の優先順位付けを自動化することを許可し、トリアージを改善します。これらのアラームだけでなく、アナリストが調査を希望する他のアラートについても、McAfee Investigator は疑いのある攻撃で収集したアラート、アクティビティ、証拠、および情報を収集、整理、要約、可視化します。

主な利点

- **持続時間の短縮：** ケース データの徹底的な調査によって、症状を修復するのではなく、根本的な原因を検出できるようにします。
- **アラートからケースへのシフト：** 優先度の低いマニュアル調査に費やされる時間を減らします。
- **未知のものに注目：** 人間の解釈や判断が必要とされるユニークな生成物と分析に焦点を絞ります。
- **トリアージの改善：** より多くのケースをより迅速かつ正確に処理します。
- **アナリストの苦労を削減：** 限られた時間、エネルギー、および認知能力を最大限に活用します。
- **アナリストのスキルの構築：** ガイドブックや関連分析により、ワークフロー内の適切な疑問と仮説についてアナリストを教育します。
- **現在のシステムの価値の拡大：** 既存のデータソースと分析を強化して、照準と精度を高めます。

関連するデータはバックグラウンドで収集され、決定をトリガーする特定の脅威の調査に重要な分析のみが含まれています。セキュリティ情報とイベント管理 (SIEM) ソリューションからのデータは、すべてのノードでエンドポイント検出 / 対応 (EDR) エージェントを必要とせずに、エンドポイントのデータで補強できます。このモデルにより、部門ごとに異なる手法に代わって、IoC、戦術、技術、手順、および関係のコンテキストに基づく可視性が実現します。

データ解析と機械学習エンジンは、証拠データを既知のベースラインおよび脅威情報源と比較します。生成物を処理し、重要な不審物の分析を強化します。

適切なデータを自動的に収集して優先順位付けすることで、McAfee Investigator は、アナリストがインシデントのリスクと緊急性を判断するための作業を軽減し、迅速化できるようにします。アナリストはより速く正確なトリアージを決定でき、最も重要な脅威に焦点を当てられます。

この利点は組織レベルではさらに大きくなります。アラートの確認からコンテキストに基づくケースにレベルを上げることで、アナリストはより効率的に行動できます。第 1 層のアナリストはより多くのケースを処理して、最優先のアクティビティに多くの時間を費やせます。

エキスパート システムの活用

インシデントに詳細調査が必要になると、アナリストはインタラクティブ ガイドブックを使って調査及び評価を行って、重要なポイントにフォーカスします。調査ガイドブックは筋書きのあるものでも、内容があらかじめ決まっているものでもありません。このシステムは人の思考プロセスを模倣して、最大限のスピードと正確性をもって複数の仮説検証を同時に行います。

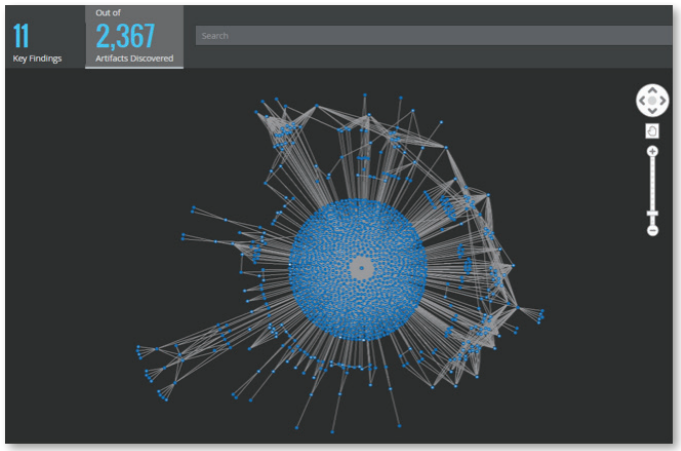

図 1. McAfee Investigator は何千もの証拠を集めます。

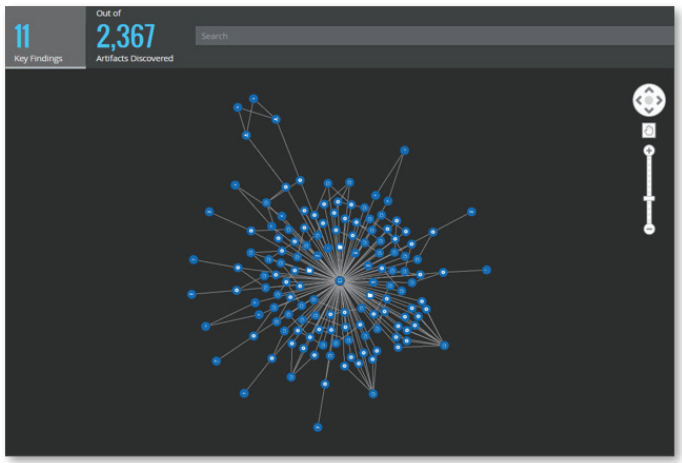

図 2. その後、McAfee Investigator は専門家の分析とアドバイスを適用して重要な発見を示します。

主な機能

- 正確なオンデマンド データ収集
- 分解可能なエンドポイント コレクション エージェント
- 専門家の指導や人工知能に基づいた収集データの解釈
- インタラクティブな可視化
- 考えられるデータを調査する様々な仮説
- 組織情報のベースライン
- ケース管理でスタッフに指示し、また調査時の情報共有を可能に

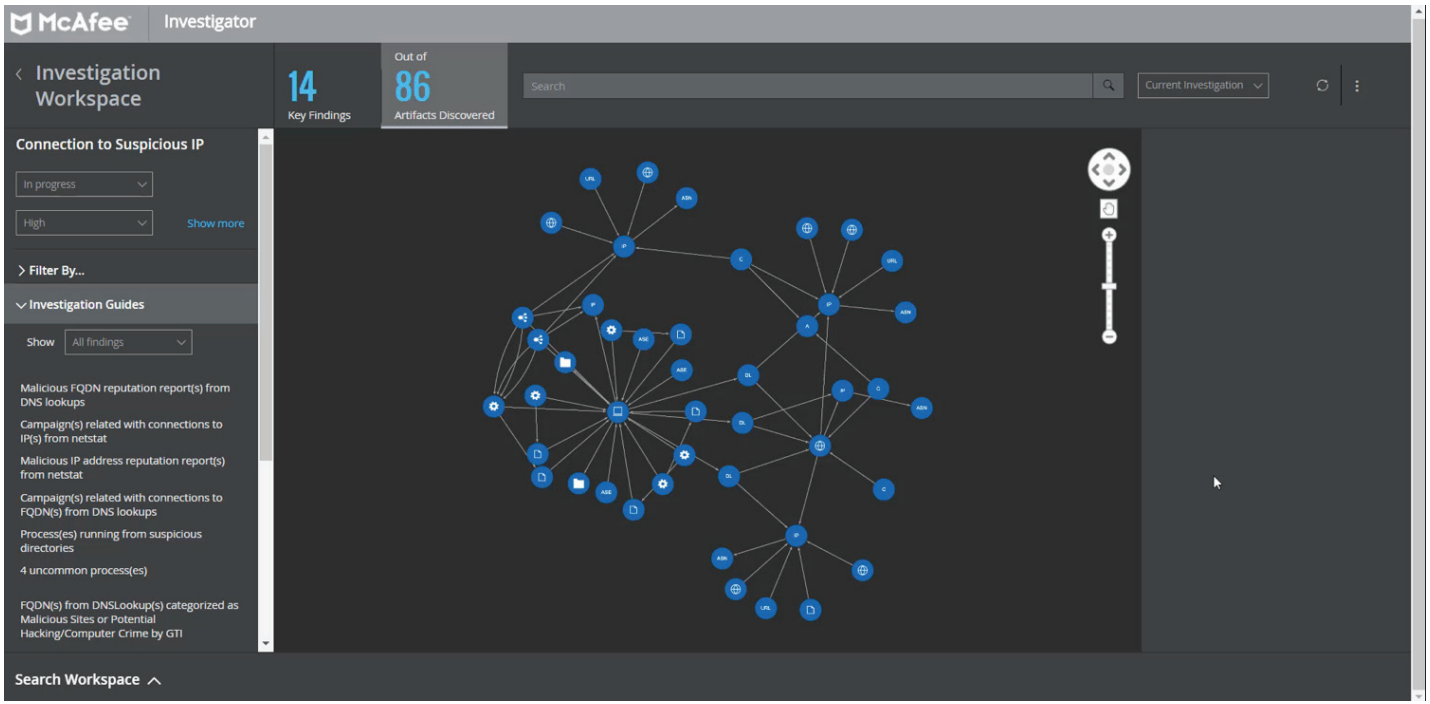

図 3. ワークスペースは、明白で調査が簡単な主な発見をまとめます。

人間が理解可能なこのガイドブックは、Foundstone® の研究者の専門知識と人工知能を組み合わせて造られました。これは、McAfee Investigator が人間と機械の能力をうまく組み合わせている一つの例です。

ワークスペースはケースの分析と発見結果を構造化し、アナリストが適切な疑問を提示するのに役立ちます。焦点を絞った、様々な角度の調査により、アナリストは高い確信をもって根本的な原因を識別し、効率的かつ正確にケースを解決できます。

膨大な情報量にも対応

McAfee Investigator のインタラクティブなワークスペースはワークフローを促し、単一の認知環境内でデータ間を移動できます。このモデルは、効率性を向上させ、多数のアラートの種類から生み出される情報負担を軽減し、複数の画面を確認する必要をなくします。

このワークスペースは、初心者および中級のアナリストに上級アナリストの思考過程を実行するように指導し、別途研修を行うことなく彼らのスキルを上げます。

既存のツールとデータを活用

McAfee Investigator は SIEM および McAfee® ePolicy Orchestrator® と協働して、既存のデータソース、ベースライン、相互関係、アラートの高度な分析を可能にします。分離可能なエージェントは、細かいエビデンスの正確な解釈に特に重要となるエンドポイント データを収集します。McAfee Investigator と McAfee Active Response の統合で、アナリストはリアルタイムでエンドポイント全体の脅威の影響を調べることができます。アクティビティ フィードはサードパーティのツールとデータを共有して現在のワークフローに繋がり、プロセスを合理化し、コラボレーションを促進します。プロフェッショナルなサービスにより、オンボーディングと有効化を促進します。

さらに詳しく

McAfee Investigator があれば、疑いがある場合にデータの収集と解釈に多くの時間をかける必要はありません。McAfee Investigator が採用する高度な分析エンジンが、コンテキスト駆動型インターフェイス内で脅威アラートを検査して優先順位付けし、セキュリティ操作を適正化します。McAfee Investigator は SOC 調査で専門家の知識を自動利用し、アナリストがよりスマートかつ迅速に正確な判断を下せるようにします。

これは人間と機械の素晴らしい連携です。

詳細については、**www.mcafee.com/jp/products/investigator.aspx** を参照してください。

〒 150-0043
東京都渋谷区道玄坂 1-12-1
渋谷マークシティウエスト 20F
Tel. 03-5428-1100（代表）
www.mcafee.com/jp