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源を自信をもって識別し、迅速に解決するのに役立ちます。優先度を付けたアラートによって、関連の SIEM とリアルタイムのエンドポイント データの調査をエキスパート レベルで開始します。セキュリティ オペレーション センター (SOC) は、マルウェア、ネットワーク脅威、および侵害の兆候 (IOC) をオートメーション、専門知識、および人工知能を使用して効率的に調べることができます。

SOC 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。

任意のインシデントを選んで調査すると、問題の核心を探るには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 SOC 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

McAfee の調査 [1] によると、熟練した SOC はオートメーションと洗練された分析を用いて根本的な原因を特定しながら迅速に解決することでこの問題に対処しています。

McAfee Investigator は、すべての SOC に高度なオートメーションと分析を提供します。SaaS のサービスと同様、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、迅速かつ簡単に評価します。

これらのインタラクティブな分析により、オートメーション、知識、および継続的に更新されるガイダンスを取得でき、インシデントの対応者がマルウェア、ネットワーク脅威、IoC を短時間で正確に完全調査できるようにします。

正確かつ迅速にトリアージを実施

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。

あるインシデントを詳細に調査することを決めると、アナリストは対象範囲の決定と評価の際に重要となる点に重点を置いたインタラクティブなガイドブックを利用します。調査ガイドブックは、スクリプトベースのものでも静的なものでもありません。システムは人間の脳を模倣し、最大速度と精度を保ちながら多くの仮説を模索します。

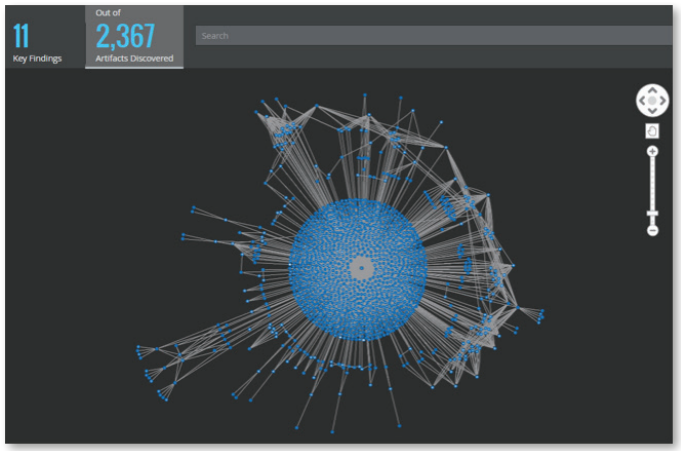

図 1. McAfee Investigator は何千もの証拠を集めます。

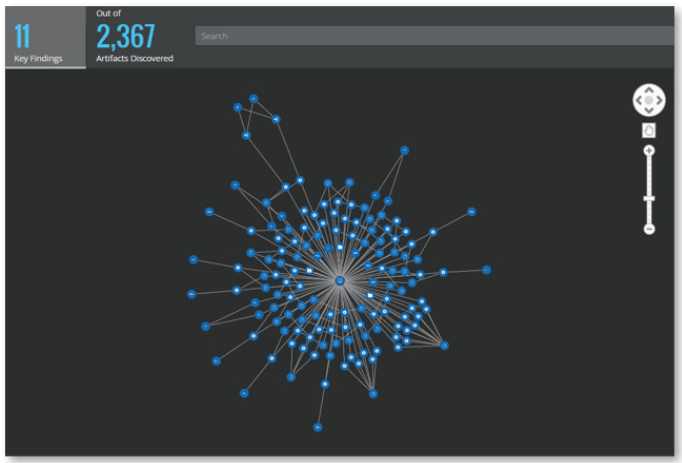

図 2. その後、McAfee Investigator は専門家の分析とアドバイスを適用して重要な発見を示します。

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
- 調査専用のケース管理

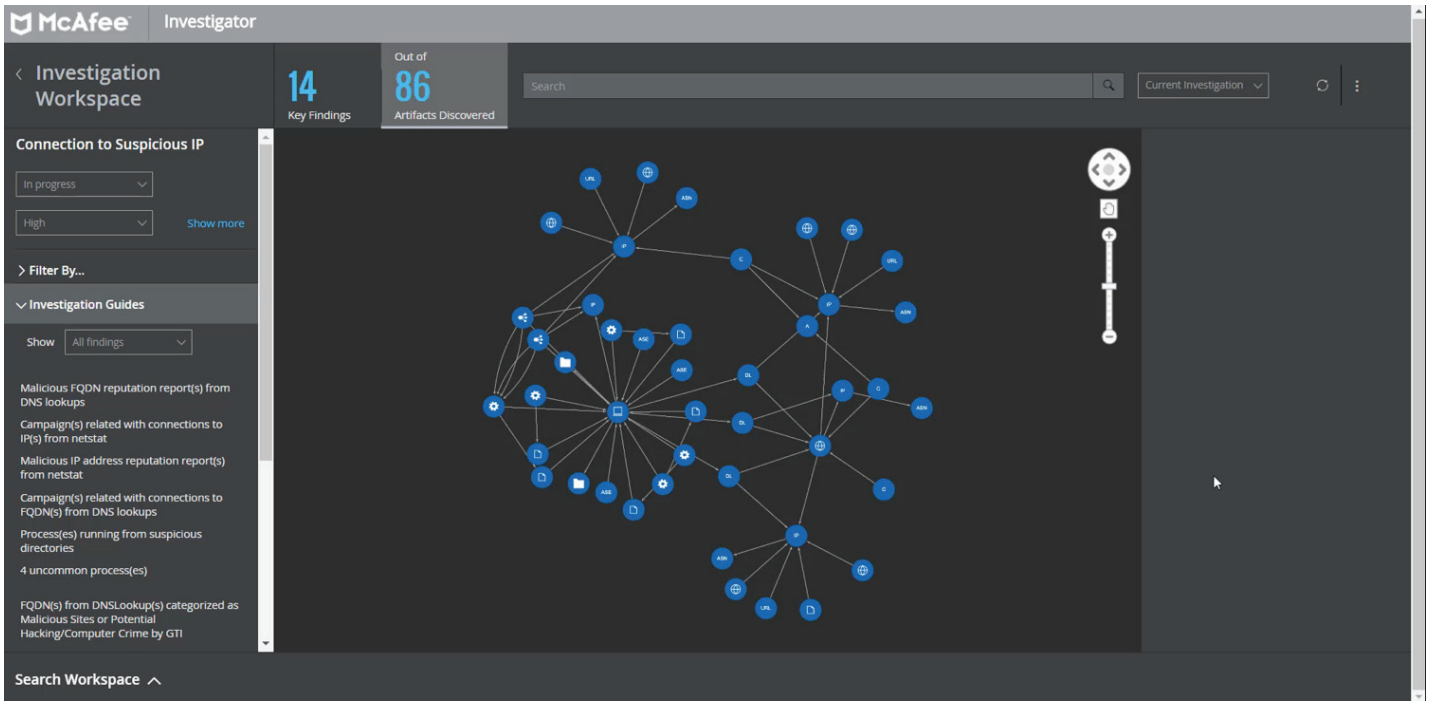

図 3. ワークスペースは、明白で調査が簡単な主な発見をまとめます。

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。

スキルと連携の強化

McAfee Investigator のインタラクティブなワークスペースは、ユーザー インターフェイスの革新を続けています。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、多数のアラートの種類から生成される情報の負担を軽減し、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。また、ケースのワークフローを有効化し、チーム全体でのケースのアクセス、記録、共有、更新を簡素化します。データの継続的な共有は、セキュリティ オペレーション センターを率いる各層と分散したチームで特に重要です。

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、アラートに高度な分析をもたらします。分離可能なエージェントが、細かい証拠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。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。

1. https://www.mcafee.com/jp/resources/reports/rp-disrupting-disruptors.pdf

〒 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