IDC ラボ検証レポート エグゼクティブサマリー

MCAFEE INTEGRATED THREAT DEFENSE SOLUTION

高度な脅威に対する分析と保護に不可欠な能力

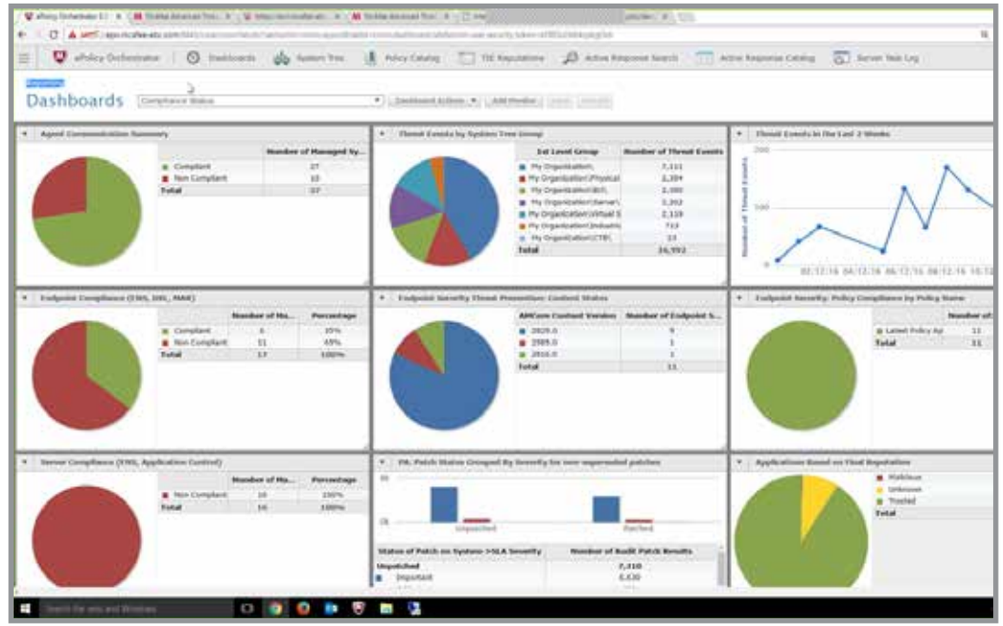
By Rob Ayoub, CISSP, IDC Security Products Team

Sponsored by McAfee | March 2017

ラボ検証レポート：エグゼクティブサマリー

IDCでは、McAfee Integrated Threat Defense Solutionを利用する以下の5つの主要なユーザー事例のシナリオの検証を行った。

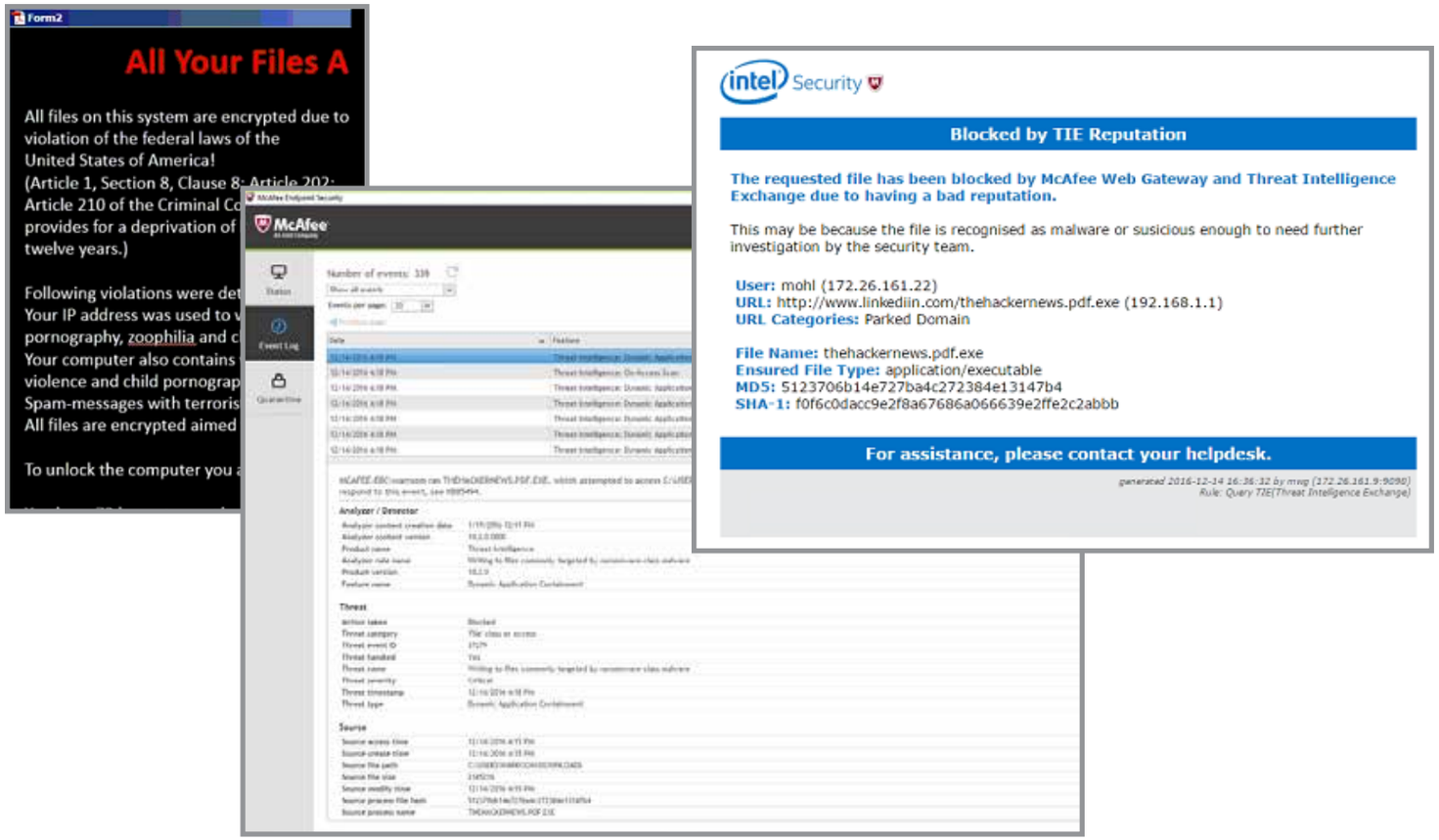
- ✔ ダイナミックエンドポイントによるゼロデイマルウェア防御
- ✔ ドライブバイダウンロードによるランサムウェアからの防御
- ✔ アプリ制御によるサーバーのマルウェア防御
- ✔ 脅威ハンティング
- ✔ IPSによるマルウェア防御



IDCの見解

McAfee Integrated Threat Defense Solutionは、統合されたセンサー、アナリティクス、インテリジェンスを自動化されたオーケストレーションに結合することによって既知または未知のマルウェアに対処する。このソリューションでは、セキュリティ専門家に対して、変化し続ける最新の脅威の検出、それに対する防御、検知に必要なすべてのツールと自動化が提供される。McAfee製品のThreat Intelligence ExchangeおよびData Exchange Layerの機能を活用することによって、セキュリティインフラストラクチャ全体が連携され、自動化されて動作し、継続的に脅威の評価を行い、存在が明確となった脅威に対して即座に対処することが可能となる。

主な検証結果：悪意のあるゼロデイマルウェアが検出され、拡散が防止された

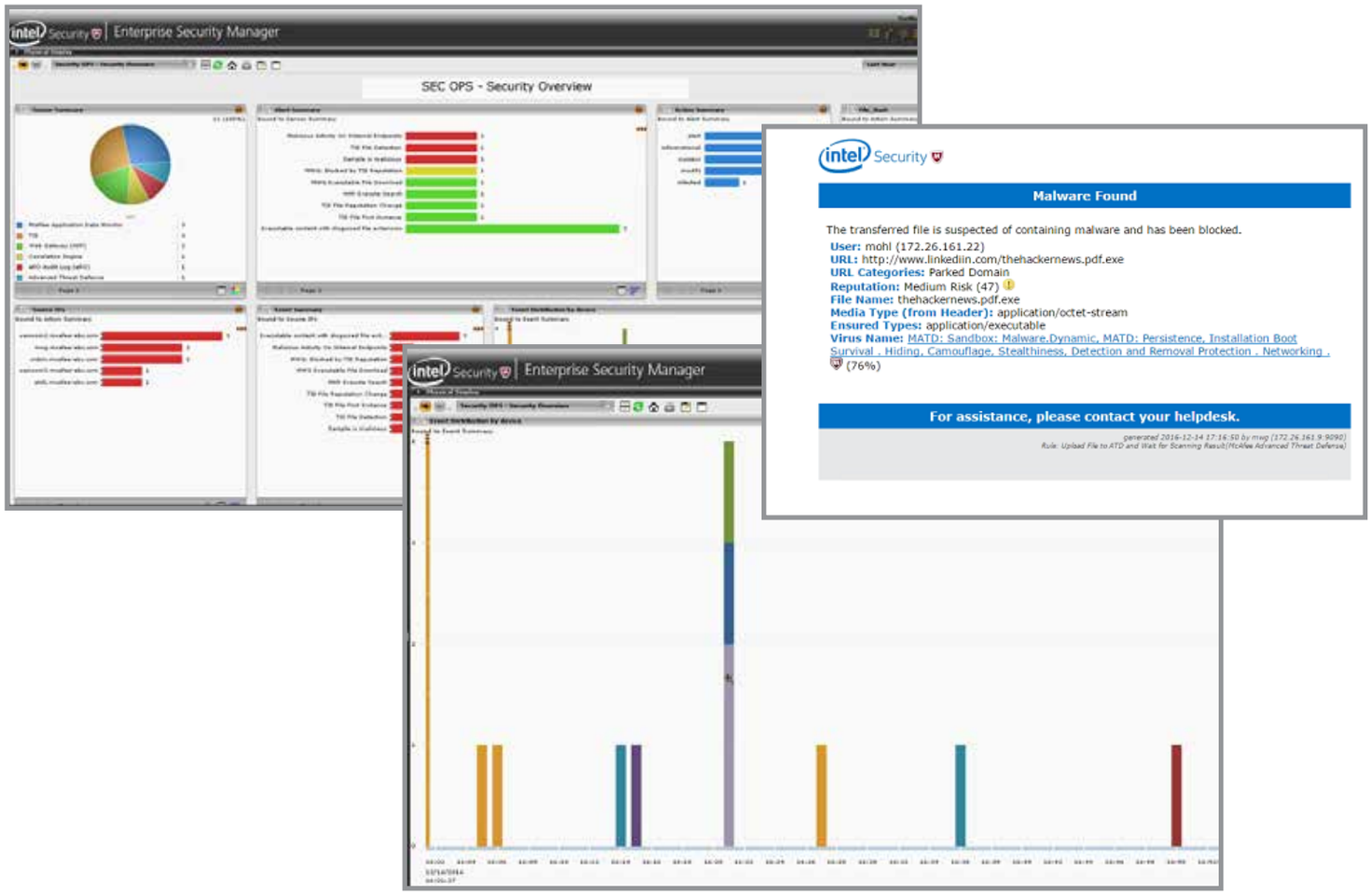


IDCの結論：IDCでは、エンドポイントクライアントによって提供されるランサムウェアに対する防御は導入と管理が容易であるという結論を得た。このシナリオ全体を通じて、高度に自動化された分析が行われた。

主要な結果：

- ダイナミックエンドポイントによって高度なマルウェアのシステムへの配信／インストールが阻止される
- ソリューションによって疑わしいファイルが自動的に分析され、不正アクセスの兆候（IOC）が生成される
- 分析ツール（ATD）にはシグネチャと挙動分析の機能がある
- ソリューションによってセキュリティ運用に対して実行可能なインジケーターが提供されるかどうか
- ソリューションによって単一のコンソールからの共通インシデントトリアージ機能が提供される（SIEM）

主な検証結果:ドライブバイダウンロードが検知され、拡散が防止された

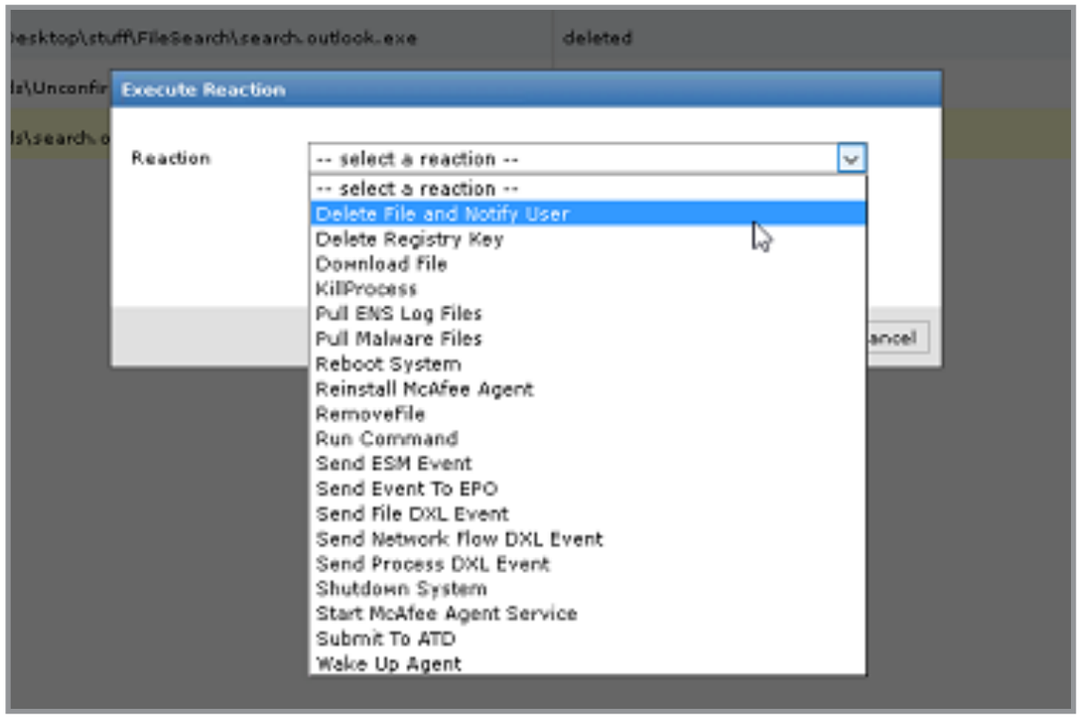


IDCの結論:ドライブバイダウンロードを防止する場合、多くのソリューションでは手作業による介入が必要である。McAfee Integrated Threat Defense Solutionでは潜在的に危険な状況に対する評価と対処が大幅に自動化されている。

主要な結果

- Web Gatewayによってスピアフィッシングを通じて実行される高度なマルウェアを阻止することが可能である
- ソリューションによって疑わしいファイルが自動的に分析され、不正アクセスの兆候(IOC)が生成される
- 分析ツール(ATD)にはシグネチャと挙動分析の機能がある
- ソリューションによってセキュリティ運用に対して実行可能なインジケーターが生成されるかどうか
- ソリューションによって単一のコンソールで読み取り可能な共通インシデントトリアージ機能が提供される

主な検証結果：アプリケーション制御による サーバーのマルウェア防御

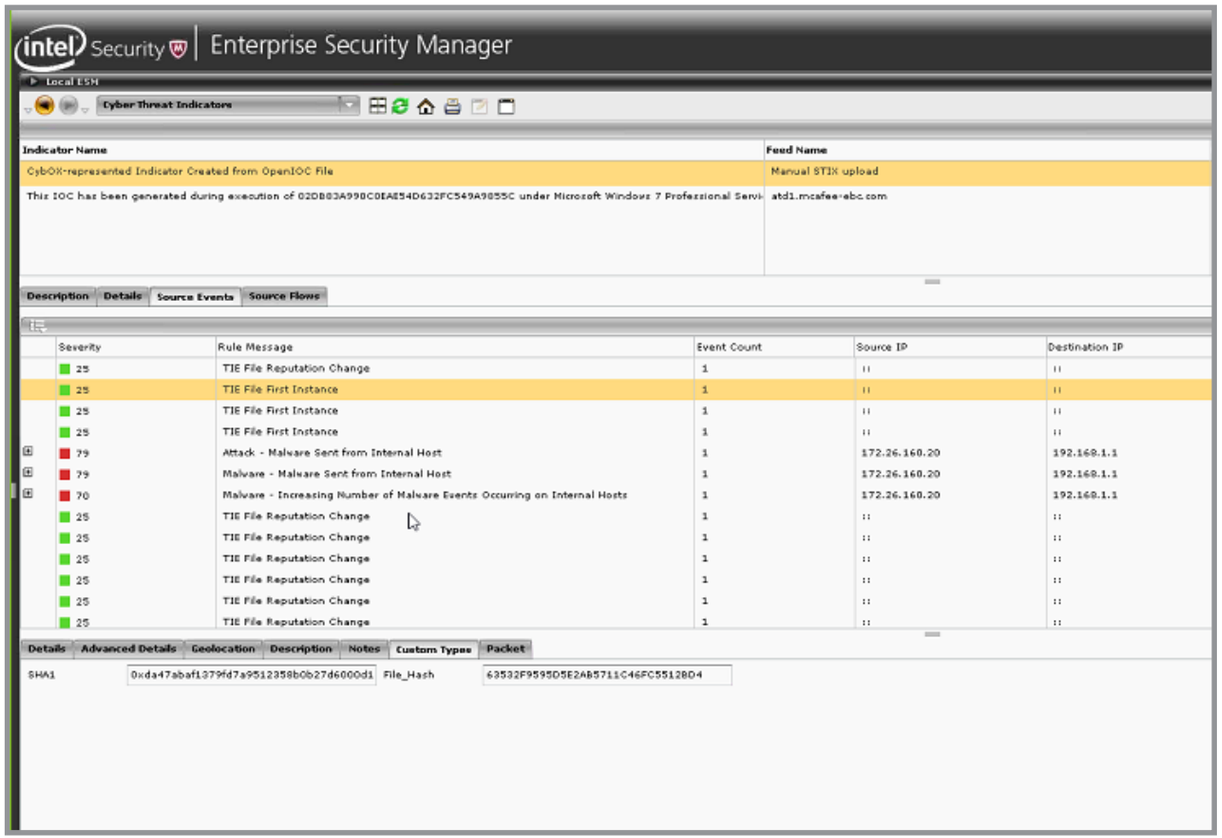


IDCの結論：アプリケーション制御によって自動化されたポリシーの設定が可能になり、企業の最も機密性の高い資産（アプリケーションサーバー）が保護できる。

主要な結果

- ダイナミックエンドポイントによってホワイトリストに登録されたサーバーを悪意のあるソフトウェアから守ることが可能である
- ソリューションによって疑わしいファイルが自動的に分析され、不正アクセスの兆候（IOC）が生成される
- 分析ツール（ATD）にはシグネチャと挙動分析の機能がある
- ソリューションによってセキュリティ運用に対して実行可能なインジケーターが生成されるかどうか
- ソリューションによってエンドポイント検知／対処機能が提供される（Yes/No）
- 単一のコンソールで読み取り可能なインシデントトリアージ機能

主な検証結果：脅威ハンティング

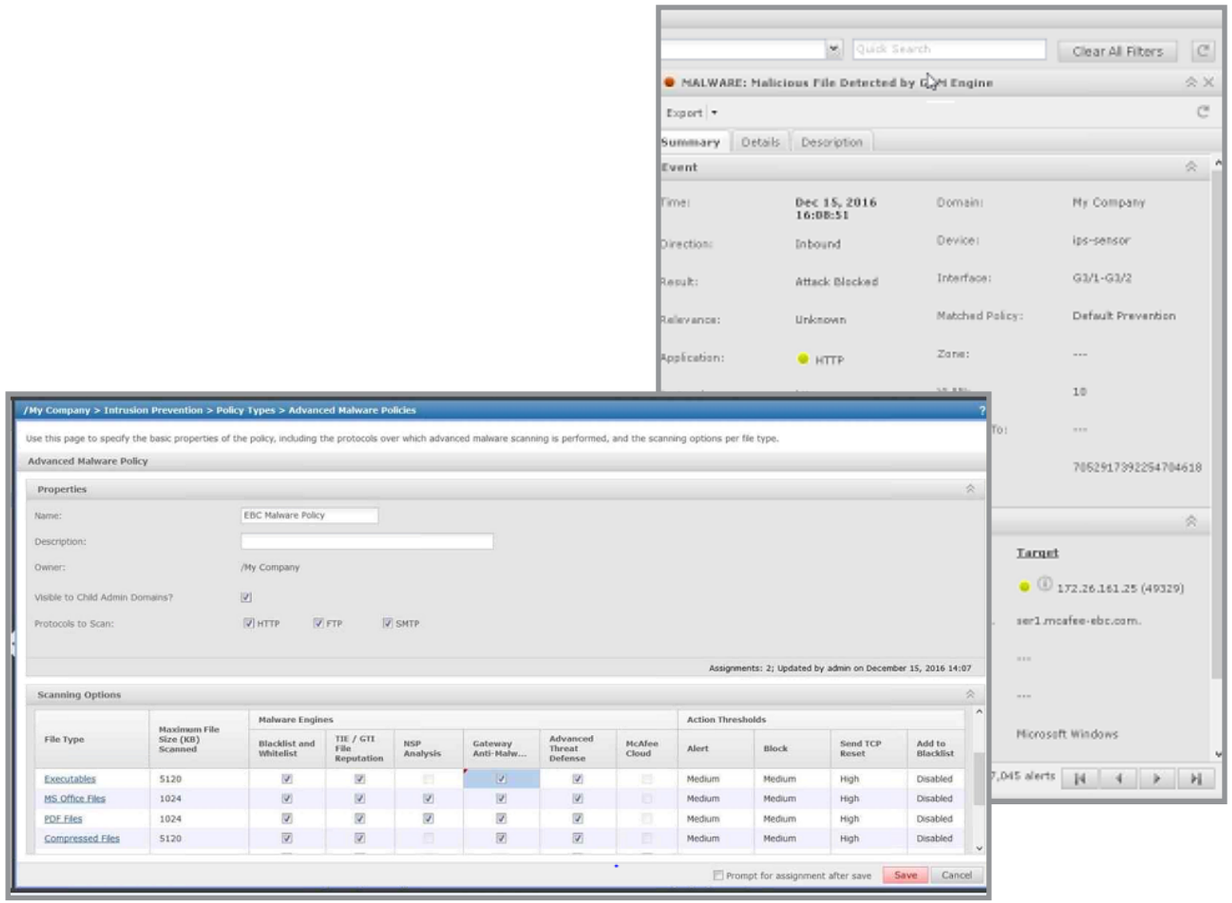


IDCの結論：マルウェアハンティングはインシデント対応の重要な要素となっている。インシデントの幅と範囲を理解する責任は企業が負っている。McAfee Integrated Threat Defense Solutionでは、アナリストが侵害の範囲を突き止めることを支援する広範な検索機能が提供されている。

主要な結果

- ソリューションは自動的に不正アクセスの兆候（IOC）を解析することが可能である
- ソリューションによってエンドポイントの検出と対処機能が提供される
- ソリューションによって単一のコンソールで読み取り可能な共通インシデントトリアージ機能が提供される（…％自動化、…％読み取り可能）
- ソリューションによってネットワークおよびエンドポイントの防御全体に渡ってインテリジェンスが共有される
- ソリューションによって自動的に不正アクセス兆候（IOC）を検索することが可能である
- ソリューションは不正アクセスの兆候（IOC）に基づいて攻撃を防止することが可能である

主な検証結果：IPSによるマルウェア保護



IDCの結論：IDCでは、エンドポイントクライアントによって提供されるランサムウェアに対する保護は導入と管理が容易であるという感触を得た。このシナリオ全体を通じて、高度に自動化された分析が行われた。

主要な結果

- IPSによってスピアフィッシングで実行される高度なマルウェアを防止することが可能である
- ソリューションによって疑わしいファイルが分析され、不正アクセスの兆候（IOC）が生成される
- 分析ツール（ATD）にはシグネチャと挙動分析の機能がある
- ソリューションによってセキュリティ運用に対して実行可能なインジケーターが生成されるかどうか
- ソリューションによってエンドポイントの検出と対処機能が提供される
- ソリューションによって単一のコンソールで読み取り可能な共通インシデントトリアージ機能が提供される（…％自動化、…％読み取り可能）
- ソリューションでは分析ツールとEDRツール間のワークフロー統合機能が提供される
- ソリューションではWeb Gatewayと分析ツール間のワークフロー統合機能が提供される（Yes/No）
- ソリューションでは分析ツールとSIEM間のワークフロー統合機能が提供される
- ソリューションではリモート修復機能が提供される
- ソリューションによってネットワークとエンドポイントのセキュリティが適用され、同一のベクトル上での将来の攻撃を防御する

検証プロセス

IDCはオランダのMcAfeeのラボで検証を実施した。テストベッドはIPS、SIEM、Endpoint、Server、Secure Web Gateway、ATD、TIEを含む広範なマカフィー製品で構成されている。各々の機能は異なる構成とテストベッド環境を使用して独立して検証された。

IDCラボ検証の分析手法

本Lab Validation BriefはIDCがサプライヤーのチームとの協力の下で実施した広範な検証プロセスの要約を提供するものである。IDCはサプライヤーの設備、施設、構成に依拠してこの検証を実施した。すべてのテストは1人以上のIDCアナリストの立ち合いの下で実施されている。

本調査レポートは、ここで検証された製品およびサービスの機能に対してさらなるデューデリジェンスの実施を望むITユーザーと意思決定者に対して、簡単な示唆と洞察を提供するものである。ただし、本調査レポートは詳細で実践的なテスト計画の策定や検証作業を行うことを目的としたものではない。これは、大半の企業が製品やサービスの購入を決定する前に実施する評価プロセスに代わるものではない。

この理由から、本調査レポートは製品のすべての機能に関する網羅的な資料を企図したものではなく、製品の代表的な特徴／機能、従来の環境との比較による相対的なパフォーマンス、そしてHadoopのワークロードにおける一定の問題の解決を望んでいる企業に対して、これらの機能が提供する価値に焦点を合わせた簡潔な資料を企図したものである。

また、本調査レポートは企業の後援を受けた資料であるが、これは製品、サービス、あるいは後援サプライヤーに対するIDCの推奨を意味するものではない。IDCの見解は独自のものであり、本調査資料の制作から影響を受けたものではない。

検証のテストベッド

この表は、検証された各々の機能に関するテスト環境の詳細をまとめたものである。

脅威防御機能	検証された脅威の防御ステップ数	自動化レベル	DXL の統合	製品コンポーネント
攻撃の検出と初期の隔離	3	100%	○	• McAfee Endpoint Security (ENS 10.2)
	4	100%	○	• McAfee Network Security Platform (NSP 8.3.7.7)
	4	100%	○	• McAfee Web Gateway (MGW 7.6.2.6)
脅威インテリジェンスの検証	4	75%	○	• McAfee Threat Intelligence Exchange (TIE 2.0.1)
				• McAfee Global Threat Intelligence
デトネーション分析	7	100%	○	• McAfee Advanced Threat Detection (ATD 3.8)
ヒストリカル分析（範囲）とその対処	4	75%	○	• McAfee Enterprise Security Manager (ESM 9.6 (10.0))
	2	50%	○	• McAfee Active Response (MAR 1.1.0)

IDCの提言

ユーザー企業への提言：情報セキュリティ最高責任者（CISO）の安眠を妨げるいくつかの重要な問題が存在する。絶え間なく変化する攻撃の状況、自社が新聞の一面記事の材料になる可能性、適格なセキュリティ人材の発見と維持の困難さは、規模の大小を問わずすべての企業にとって最大の課題となっている。

しかし、ビジネスを中断することは許されないため、企業は何らかの対処をしなければならない。これらの課題に対する回答は、あらゆるベクトルに渡る既知および未知の攻撃を常に監視、分析し、それらから保護する統合的なアプローチによってセキュリティを強化することである。さらに、このソリューションは、アナリストが彼らの最も基本的な業務を自動化することを可能とするインターフェースと検索機能を備え、アナリストに対して潜在的な侵害の発見、侵害の発生の有無の判断、インシデントの拡散範囲の評価および修復のために必要なツールを提供できる必要がある。

これらのすべての課題に対処するソリューションは、ある特定の攻撃ベクトルに限定された最善のソリューションであってはならず、広範で多様な攻撃プラットフォーム全体に渡って迅速に効果を発揮する必要がある。CISOの睡眠を改善できるソリューションは、物理、仮想、クラウドなど、インフラストラクチャ全体に渡って統合されなければならない。このソリューションでは、エンドポイントに至るまでネットワーク全体を「見る」必要がある。このソリューションでは、ファイルがダウンロードされたときやネットワークを移動したときに、ファイルの履歴を提供できる必要がある。今日の脅威状況に対処するために必要なすべての機能を提供できる単一のポイントソリューションは存在しない。

コミュニケーションと情報の配信もCISOの最重要課題に対処するために必要な主要機能である。統合ソリューションのすべてのコンポーネントは、セキュリティアナリストおよびネットワーク内の他のコンポーネントに対して、迅速かつ自動的に情報を伝達できる必要がある。これが、緩慢で煩雑な手作業による調査に依存する必要なく脅威を阻止できる唯一の方法である。

IDCの提言（続き）

McAfee Integrated Threat Defense Solutionは上述のすべての課題に対処している。このソリューションでは、統合されたセンサー、アナリティクス、インテリジェンスを自動化されたオーケストレーションに結合することによって既知または未知のマルウェアに対処している。McAfee DXL対応のラボによって、平均して8分間のオーケストレーションされた脅威対応において、以下の統合／自動化が図られる。

- 25種類の脅威トリアージのステップ
- 3つの脅威保護プラットフォーム（エンドポイント、Webおよびネットワークのセキュリティ）：ファイル、アプリケーション、Webおよびネットワークの脅威ベクトルをカバー
- 3つのセキュリティアナリティクスエンジン（MAR、ESM、ATD）：リアルタイムかつヒストリカルな、詳細なマルウェア分析をカバー
- 9種類の脅威インテリジェンスのチェック

このソリューションではインフラストラクチャ全体に渡ってポリシーに基づく保護が提供される。このソリューションでは、潜在的に悪意のあるファイルの評価、これらのファイルが脅威を提起するか否かの最終的な判断、そしてこれらのファイルの適切な修復を行うためのアクションが自動的に行われる。McAfee Integrated Solutionでは、セキュリティアナリストがネットワークの深部まで掘り下げるために使用できる豊富な調査ツールが提供されており、アナリストは不正アクセスの兆候（IOC）および攻撃者が盗もうとする重要なデータを探す際に残す可能性のある痕跡を理解することが可能である。McAfee Integrated Threat Defense Solutionはセキュリティチームを強化できるように設計されている。McAfeeが提供しているカバー範囲の深さを持つベンダーはほとんどなく、セキュリティチームが直面する可能性のあるシナリオの多様性を考慮すると、統合システムのメリットは明確である。