McAfee Active Response

インシデントレスポンスを効率化する検出、監視、対応

セキュリティを重視する多くの企業では、劇的に変化する脅威への対応が問題となっています。攻撃はこれまでにない速さで増加し、増殖しています。特定組織を狙うDesigner攻撃では、検出を回避して成功率を高めるため、組織固有の情報を使用した標的型攻撃が行われました。侵入防止技術が回避され、侵入を許すケースも少なくありません。この課題に真剣に取り組んでいる企業は、検出能力が高く、調査と復旧を迅速に実行できる統合ツールを探しています。検出能力と対応能力に優れたソリューションがあれば、システムの数や情報量が増えても、効果的なセキュリティ対策が可能になります。McAfee® Active Responseは、既存のセキュリティ管理ソリューションに簡単に統合し、操作も簡単です。

攻撃の機会を大幅に減らし、組織のコンピューティング資産と企業ブランドを守ることができます。

主な特長

- **自動化：**コンテキスト情報を収集し、システムの状態を常時監視します。IoAの可能性がある変更や潜伏している攻撃コンポーネントを検出し、分析、運用、フォレンジックの各チームに脅威情報を送信します。
- **適応性：**警告を受けたときに、攻撃の状況に合わせてデータの自動収集、アラート、対応方法を調整できます。また、顧客のワークフローに合わせて設定をカスタマイズできます。
- **継続性：**攻撃イベントを検出すると、コレクターがトリガーを実行し、ユーザーとシステムに攻撃を警告します。

変化の激しい脅威状況

どの企業も攻撃を受ける可能性があります。攻撃を早期に検出するだけでなく、実行中のアクティビティや攻撃の兆候（IoA）を検知し、これらの脅威に迅速に対応できるように準備する必要があります。しかし、現在の可視性、検出、対応能力では十分な対応ができません。この課題を解決するには新しい技術が必要です。

現在のインシデント対応の限界

組織で発生した不審なイベントや既知のインシデントを調査する場合、インデント対応担当者とセキュリティ管理者は時間と規模の制約を受けます。既存のシステムやツールが収集する大量の情報を分析するには、膨大な時間がかかります。データ収集では速度が重要な要素となりますが、収集されたデータや対象のシステム数を考えると、分析に時間がかかるのもやむを得ません。また、膨大なデータから意味のある重要な情報を見つけ出すことは簡単ではありません。

インシデント対応では担当者自身が作成したスクリプトが調査で使用されるのが一般的です。これらのツールは、広範囲な分析ができるようにデータを収集します。このアプローチはよく用いられますが、組織全体の状況を迅速に把握するには限界があります。組織で特定のIoAを迅速に調査できないため、適切な対応ができない場合も少なくありません。時間的な制約から調査を意図的に制限することもあり、インシデント対応プロセスで重大な欠陥となる可能性もあります。現在使用しているツールの制約で作業が制限されてしまうのは大きな問題です。

システム要件

ハードウェア最小要件

サーバーは仮想マシンにもインストールできます。McAfee Active Responseサーバーの最小ハードウェア要件は次のとおりです。

- 4コアIntel® Xeon® CPU X5675、3.07 GHz
- 8 GB以上のRAM
- 120 GB SSD

サービスに必要なインフラ

- McAfee® ePolicy Orchestrator 5.1.1 以降
- McAfee Agent 5.0 以降の拡張ファイル
- McAfee Data Exchange Layer2.0.0.430 以降のブローカー

対応Webブラウザー

- Microsoft Internet Explorer 9以降
- Google Chrome 17以降
- Mozilla Firefox 10.0以降

クライアントに必要なインフラ

- McAfee Agent 5.0.2.132以降（Windows 10）
- McAfee Agent 5.0.0.2620以降（Windows 10以外）
- McAfee Agent 5.0.0.2710以降（Linux）
- Data Exchange Layer 2.0.0.430以降のクライアント（全ての管理対象エンドポイント）

包括的な検出と対応

McAfee Active Responseは、高度なセキュリティ脅威を継続的に監視し、対応を行います。最先端の検出技術、詳細な分析、フォレンジック調査、総合的なレポート、優先順位が設定されたアラートとアクションにより、セキュリティ状況を監視できます。脅威の検出率だけでなくインシデント対応能力も向上します。エンドポイントにおける検出と対応（EDR）の厳密な要件に対応するため、McAfee Active Response は事前定義のコレクターとカスタマイズ可能なコレクターを使用して、すべてのシステムでIoAを調査します。実行中のプロセスに存在する痕跡だけでなく、潜伏している脅威や削除された可能性のある脅威も検出します。McAfee Active Responseは現在のIoAだけではなく、今後発生するIoAに対しても目的に合わせて警告とアクションを実行します。

McAfee Active Responseは、Intel Securityの統合セキュリティ アーキテクチャの有効性を証明します。複雑な環境でも、より多くの脅威をより少ないリソースで迅速に解決できます。McAfee Active Responseを利用すると、エンドポイントの可視性を維持し、詳細な調査が可能になるので、侵害をより速く認識できます。また、業務に支障をきたさずに問題を迅速に解決できるツールも用意されています。これらの機能はすべてMcAfee Data Exchange Layerを介してMcAfee® ePolicy Orchestrator®（McAfee ePO™）で管理されます。拡張性に優れた統合環境が用意されるので、製品を管理する要員を増やす必要もありません。

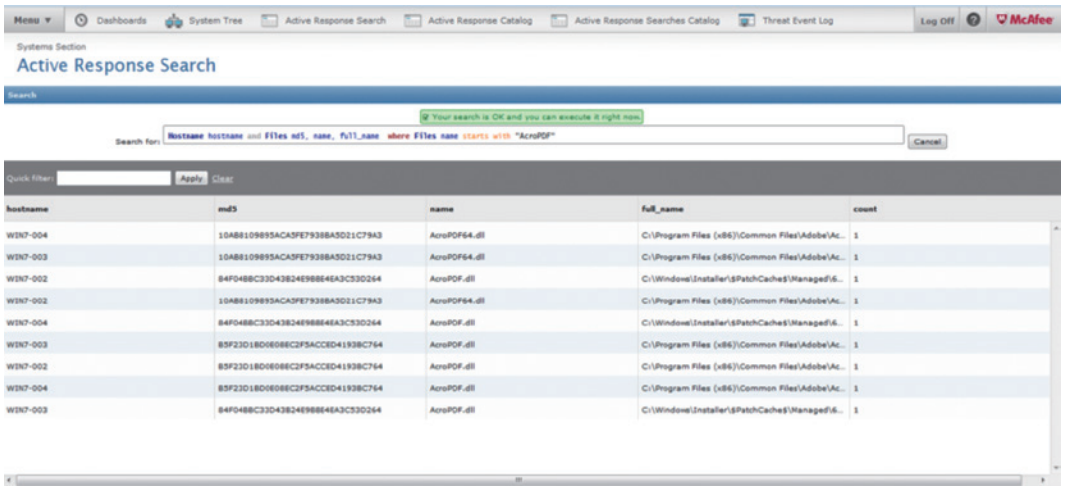

表1. McAfee Active Responseの検索インターフェース

対応クライアントOS

- Microsoft Windows
  - Windows 10 Enterprise (32-bit/64-bit)
  - Windows 8.0 Base (32-bit/64-bit)
  - Windows 8.1 Enterprise Base U1 (32-bit/64-bit)
  - Windows 2012 Server Base R2 U1 (64-bit)
  - Windows 2008 R2 Enterprise SP1 (64-bit)
  - Windows 2008 R2 Standard SP1 (64-bit)
  - Windows 7 Enterprise SP1以前 (32-bit/64-bit)
  - Windows 7 Professional SP1以前 (32-bit/64-bit)
- CentOS 6.5 (32-bit)
- RedHat 6.5 (32-bit)

機能	ポイント	メリット	特長
検索(コレクター)	システムからデータを検索し、表示します。	コレクターの検索機能により、システムを詳しく調査できます。システムから収集されたデータがビジュアルに表示されるので、重大な侵害や攻撃の可能性を確認できます。一般的なスクリプト言語に対応しているので、独自のコレクターとリアクションを作成し、最適な処理を行うことができます。	McAfee Active Responseは、実行ファイルだけでなく実行中のファイルに潜伏するコードや攻撃の痕跡を消すために削除された可能性のあるコードも検出します。McAfee Active Responseは、ファイル、ネットワーク フロー、レジストリ、プロセスを検索できます。
監視(トリガー)	セキュリティ担当者が重大なイベントやシステム変更を継続してモニタリングできます。1つのトリガーで現在と将来のイベントに対応できます。	設定したトリガー条件を満たすと、アクションが実行され、イベントが生成されたり、リアクションが実行されます。McAfee Active Responseはピーク時を避けて応答モードを継続して維持できます。	McAfee Active Responseでは、今日見つかったウイルスだけでなく、今後発生する可能性がある脅威にもアクションを実行できます。
対応(リアクション)	トリガー条件を満たしたときに実行される処理が事前に設定されています。これにより、脅威を検出し、駆除できます。	ファイル ハッシュ(MD5とSHA1)により、システムから削除されたファイルを検索できます。ホストが現在接続しているIPアドレスや過去にアクセスしていたIPアドレスを確認できます。また、システムでアクセスされていないPE以外の不正なファイルを検索できます(ファイル システムにコピーされ、まだ開かれていない不正なPDFを検索します)。	McAfee Active Responseは、検索結果に対してアクションを実行するように設定されています。また、特定の要件に合わせてカスタム アクションを設定することもできます。
McAfee ePOによる一元管理	1つのコンソールで総合的な管理作業を行い、処理を自動化できます。	Intel Securityの統合セキュリティアーキテクチャの一部としてMcAfee ePOを利用することで、脅威の検出、対応、回避を自動的に行うことができます。1つのウィンドウで全体のセキュリティ状況を把握できます。操作が簡単で、作業時間を短縮し、負荷を軽減できます。	1つのコンソールで管理作業とアクションを実行できます。単一のコンソールでMcAfee Active Responseなどの強力なセキュリティ管理機能を実行し、様々なプラットフォームを保護することができます。
統合セキュリティアーキテクチャ	Data Exchange Layerにより、Intel Securityの他のマカフィー製品との通信が簡単になります。	Intel Securityの統合セキュリティアーキテクチャの一部として、McAfee Active Responseはリスクを軽減し、対応時間を短縮します。このプラットフォームの革新的な概念、最適化されたプロセス、実用的な推奨事項により、オーバーヘッドと運用コストを削減できます。	

McAfee Active Responseの詳細については、**http://www.mcafee.com/jp/products/active-response.aspx**をご覧ください。

マカフィー株式会社 www.mcafee.com/jp

東京本社	〒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)	FAX:03-5428-1480
西日本支店	〒530-0003 大阪府大阪市北区堂島2-2-2 近鉄堂島ビル18F	TEL:06-6344-1511(代)	FAX:06-6344-1517
名古屋営業所	〒450-0002 愛知県名古屋市中村区名駅4-6-17 名古屋ビルディング13F	TEL:052-551-6233(代)	FAX:052-551-6236
福岡営業所	〒810-0801 福岡県福岡市博多区中洲5-3-8 アクア博多5F	TEL:092-287-9674(代)	

MCADS_MAR-1601-GRP