Security Connected 参照アーキテクチャ
Technology Blueprint

高度な標的型攻撃への対抗：検知

高度な標的型攻撃への対抗に関するブループリント 3 部作のパート II

intel Security

Intel Securityは、高度な標的型攻撃を阻止するため、3つの方法で対処することを推奨しています。この文書では、異常な行動を検知し、長い間見過ごされる可能性がある捉えにくい攻撃を発見するための高度な監視について説明します。攻撃の証拠が明らかになったら、この攻撃情報をシステム間で共有し、セキュリティインフラストラクチャ全体の意思決定能力を高める必要があります。全体像を把握するためには、Protect（防御）とCorrect（復旧）のブループリントをご覧ください。

影響が及ぶ前に高度な脅威を検知する

状況

侵害や活発な攻撃が検知されずに数カ月間継続され、数カ月、あるいは数年も明らかにならないケースが続発しています。企業がデータ損失の発生を知るのは、たいてい顧客や警察などの第三者に通知されたときです。こうした状況に遭遇したことがない企業も、インシデント検知に対するアプローチを変えなければ、いずれこの事態に直面することはわかっているはずです。侵害を発生と同時に発見するにはどうすればよいでしょうか。セキュリティ担当者はこの疑問に対する最善の回答を見つけ出す必要があります。

懸念の拡大

最大の問題は、「現在攻撃者が環境内に存在するか」という質問に回答できるかどうかです。攻撃とインシデントの検知は、非常に高度な訓練を受けているセキュリティ担当者にとっても困難な作業です。以下にその理由を示します。

- **可視性の欠如。**従来のセキュリティソリューションはサイロ化されています。各製品はセキュリティ全体の一部をなしていますが、全体像は誰にも把握できません。したがって、高度な攻撃を明確に特定するために必要なデータの収集は、セキュリティチームにとって困難で時間がかかる作業になっています。セキュリティチームが不審な動きを見つけたら、セキュリティアナリストは複数のコンソールにログインして必要なデータを取得したり、関連情報を保持する他のチームと接触したりするために、数時間から数日を費やす場合があります。
- **不要な情報が多すぎる。**セキュリティデータが爆発的に増加したため、ログの収集では膨大なデータに対応しなければなりません。環境を構成する多くのポイント製品やアプリケーションからは、毎日数百万件のイベントが発生しています。イベントが発生するたびにアラートを受信していたら、アラート疲れに陥ってしまい、結果として重要な兆候を見落としかねません。しかしイベントを無視しすぎると、攻撃全体を見逃してしまう可能性があります。
- **攻撃の高度化。**高度な標的型攻撃の大半は、ステルス性が高いため検知が困難です。こうした攻撃は、多くの感染媒体、高度な検知回避技法、モーフィングメカニズムを駆使して検知されずに環境に留まります。侵害の指標（IoC）は捉えづらく、検知が困難になることがあります。また、IoCを1つ検知したからといって隠された脅威をすべて検知したというわけではなく、この脅威が異なる形態に変化して戻って来ないとも限りません。
- **時間との闘い。**攻撃と検知するまでの時間と攻撃による損害の度合いには、明らかな相関関係があります。だからこそ侵害の検知では時間が極めて重要です。検知が早いほど、迅速に対応することができます。損害発生前に攻撃を阻止し、封じ込めるためには、「ゴールデンアワー」（最初の侵害直後の時間）中に侵害を検知することが不可欠です。残念ながら、セキュリティチームの大半は、現在使用しているソリューションではタイムリーに侵害を検知できません。インシデントの発生直後ではなく、数日、数週間、あるいは数カ月かかることさえあります。

ソリューションの説明

損害の発生前に高度な標的型攻撃を検知する鍵は、可視性、セキュリティインテリジェンス、そして継続的な監視です。ですから、環境内で発生しているイベントの完全な可視性を継続的に提供し、そのデータに最新のセキュリティインテリジェンスを適用できるソリューションが必要です。最もタイムリーな検知を行うために、このソリューションは環境内でのイベントの発生と同時に、自動的にリアルタイムでこのプロセスを発生させる必要があります。それと同時に、管理者によるプロアクティブな対応を実現するために、管理者がいつでも新しい脅威インテリジェンスを使用して環境をチェックできるようにするか、システムによるチェックを自動化しなければなりません。

高度な攻撃の検知にまず必要なのは、可視性の確保です。Intel Securityでは、中央のロケーションでセキュリティ製品と非セキュリティ製品両方から、ログとイベント、ネットワークフロー、アプリケーション、電子メール、Webトラフィック、IDなどの環境全体に関するデータを収集することを推奨します。収集するデータが多いほど、包括的で正確な全体像をつかめる可能性が高まります。

しかしデータの収集だけでは不十分です。データは活用できなければ意味がありません。データをノイズから貴重な情報に転換するには、リアルタイムの高度な分析機能が必要です。分析プロセスですべてのデータを調査して重要性の低いデータと高いデータを分離し、さまざまなソースから得られる関連イベントを相関付けてインシデントを作成し、ノイズを削減することによって、重要なインシデントの可視性を高め、重要な情報のみに焦点を当てることが理想的です。このプロセスが完全に自動化されると、リアルタイムで攻撃を検知することができます。しかし、検知の質、つまりインシデントの見逃し、誤認識の低減、アラート疲れを発生させないことも、ソリューションの調査機能に左右されます。そのため、脅威インテリジェンスにアクセスできる機能が非常に重要です。検知の質、精度、速度すべてが、脅威インテリジェンスにアクセスできる機能にかかっています。

脅威インテリジェンスは、業界のフィードやセキュリティベンダーなどのサードパーティからも取得できます。しかし、特に高度な標的型攻撃の結果を素早く得るには、社内で活用しているソリューションからも脅威インテリジェンスを取得できなければなりません。これがローカルインテリジェンスです。ローカルインテリジェンスからは、組織の通常の活動の状況、独自の環境のコンテキスト、既知または自社のセキュリティソリューションによって生成された侵害の指標を得られる必要があります。たとえば、サンドボックステクノロジの分析によってマルウェアのIoCリストが生成された場合、高度な脅威検知のためのソリューションは、これらのIoCを全体で共有し、管理者が即座に環境内のマルウェア検出を開始できるようにする必要があります。

今日は攻撃を検知できたからといって、攻撃者が過去に侵入を試みたり侵入に成功したりしていないとは限りません。ですからこのソリューションは、アラートがトリガーされる前に管理者が攻撃指標（IoA）の調査を開始できる機能を提供する必要があります。異常なイベントを観察した、ニュースやセキュリティフィードを通じて新しい脅威に関する情報が入ったなど、不審な活動が発生したときには、プロアクティブな検知が極めて重要です。こうしたケースでは、管理者がこのソリューションを通じて環境内の指標をプロアクティブに追跡し、新しい脅威によって環境が侵害されていないかどうかを確認できる必要があります。

意思決定の要素

組織のアーキテクチャーには、次のような要素が影響します。

- スケーラビリティ：どれくらいの規模の環境を監視する必要があるか
- 侵害を検出するために24時間365日体制のセキュリティインシデントチームを結成できるか
- イベントやログのデータを現在どこに保管しているか
- 環境内で1秒あたりいくつのイベントが生成されるか
- 現在どのようなログとデータを収集しているか

マカフィーのソリューションで使用されているテクノロジー

このようなソリューションを構築するために、Intel® Securityは革新的なテクノロジーを相互に統合し、過去、現在、将来の標的型攻撃を監視して検出できるよう支援しています。セキュリティ情報/イベント管理（SIEM）プラットフォームであるモジュール型のMcAfee Enterprise Security Manager、McAfee Advanced Threat Defense、McAfee Active Response、McAfee Threat Intelligence Exchangeは、損害の発生前に高度な標的型攻撃を検知するために必要なフレームワークを構成します。この4つの構成要素は連動するように統合可能で、包括的で効率的な比類のない機能を提供します。各要素は、個別に導入して、社内開発、サードパーティ製を問わず既存のセキュリティソリューションと統合することもできます。さらにその他のIntel Security製品とも統合すると、インフラストラクチャ全体の可視性が高まり、脅威インテリジェンスも拡張できます。

McAfee Enterprise Security Managerはこのソリューションの中核をなします。まずこのSIEMソリューションによって完全な可視性が提供されます。このソリューションは、完全な状況認識のために必要なデータ収集を行います。インシデントの検出に必要な次のステップとなるこのデータの分析も、高度な相関モジュールを使用してこのSIEMソリューションによって行われます。

次はMcAfee Advanced Threat Defenseが、SIEMの分析能力を高めるために、エンドポイントやゲートウェイ対策によって収集されたコンテンツとインテントペイロードや、RESTful APIを介した入力に対する深い洞察を提供します。McAfee Advanced Threat Defenseは、自社のサイト内で発見されたマルウェアや、会社と社内ユーザーを狙ったファイルから得られたインテリジェンスなど、最も正確な脅威インテリジェンスをMcAfee Enterprise Security Managerに提供します。Advanced Threat Defenseは、ゼロデイマルウェアを特定すると、このマルウェア属性と一致するIoCのリストと、このマルウェアが実行された場合に発生する変更とアクションのリストを生成します。McAfee Enterprise Security Managerは、Advanced Threat Defenseから自動的にこの情報を受信します。

次にEnterprise Security ManagerのBackTrace機能によって、過去のイベント内でIoCに一致するイベントが調査され、環境内で過去に同様のイベントが発生していた場合には管理者に通知されます。このソリューションは、アラーム機能によってそれ以降もこれらのIoCを監視します。将来同じIoCに遭遇した場合は、攻撃が再発したかどうかが即座に管理者にアラートで通知されます。

McAfee Active Responseは、環境内のIoCをプロアクティブに調査することによってMcAfee Enterprise Security Managerソリューションの機能を補完します。Active Responseは、Advanced Threat Defenseが提供するインテリジェンスも活用するので、管理者は既存のマルウェアを調査できます。Advanced Threat DefenseがIoCのリストを生成すると、インシデント対応チームと管理者はActive Responseを使用してシステム内に隠れている悪質なゼロデイファイルを探すことができます。こうしたファイルは、Advanced Threat Defenseの検知前にユーザーによってダウンロードされ、まだ実行されていない可能性があります。Active Responseは、メモリ内のアクティブなプロセスや、その他の多くのIoCも探します。即座にIoCを探すだけでなく、McAfee Active Responseはコレクタを使用してエンドポイント内の特定のIoCの存在も継続的に監視します。管理者には、環境内でIoCが見つかるとすぐに自動的にアラートが送信されます。

最後に、McAfee Threat Intelligence Exchange と Data Exchange Layer（DXL）が他のすべてのコンポーネント間にリアルタイムで脅威インテリジェンスを転送します。たとえば、Advanced Threat Defenseが環境内の既知のマルウェアの存在を突き止めると、Threat Intelligence ExchangeはDXL Layerを使用して即座にSIEMソリューションとその他のコンポーネントに通知します。リアルタイムでの脅威インテリジェンスの共有は極めて重要です。この情報共有によって、攻撃情報が生成され次第すべてのセキュリティソリューションが攻撃を検出できるようになります。

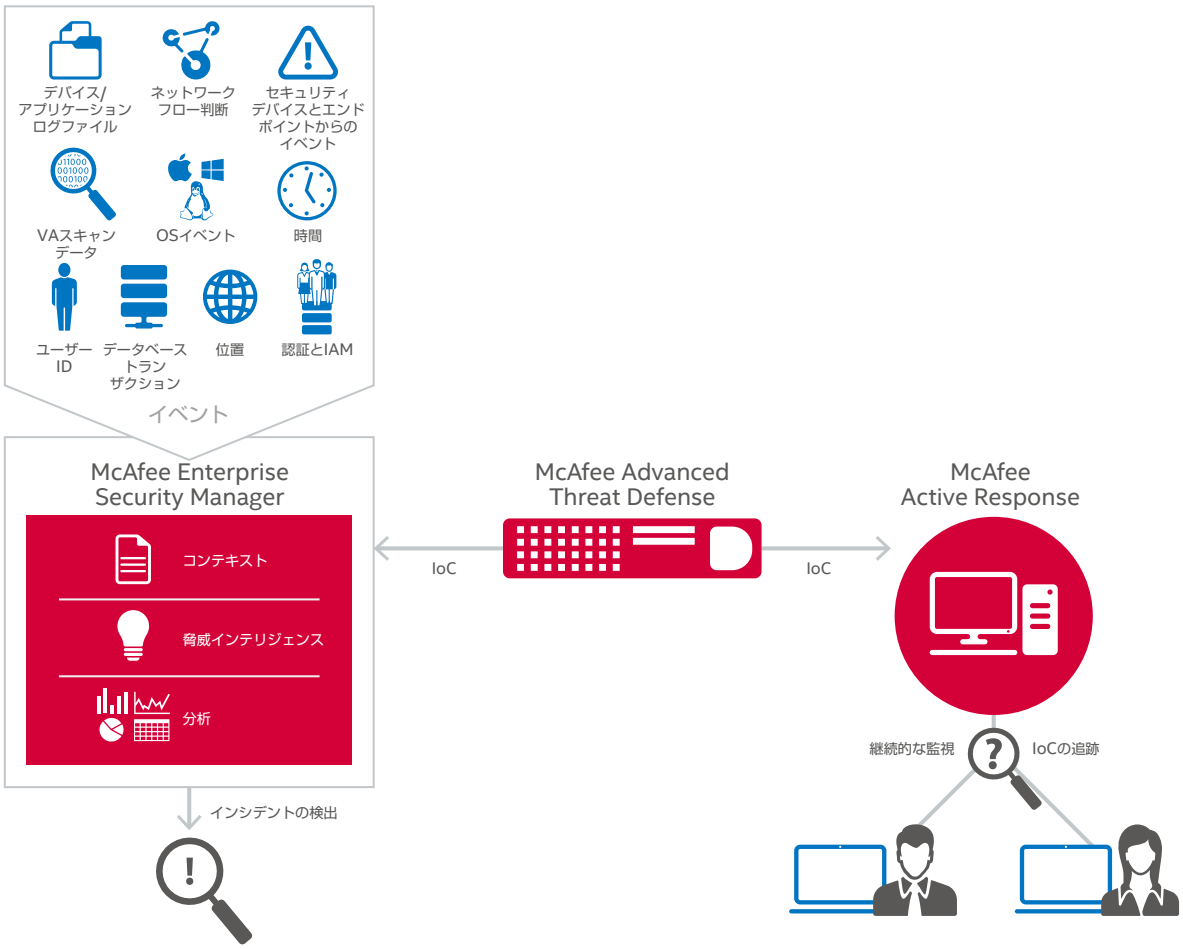

図1. Intel Securityソリューションで使用されるテクノロジー

- **McAfee Enterprise Security Managerは、完全な可視性と一元的なインテリジェンスを提供します。**このソリューションは環境内の製品から必要なすべてのイベントとデータを自動的に収集し、これらのデータの分析、相関付けを行うことにより、高度な標的型攻撃を検出します。

  まずMcAfee Enterprise Security Managerソリューションは、さまざまなソースからのイベントの収集、その正規化と統合を自動的に行い、完全な可視性を提供します。次に、ユーザー情報やホスト位置情報など、アップストリームデータソースから送信された、元のイベントには含まれていなかったコンテキストでこのデータを強化します。

  その後、ルールベースのイベント相関付けを利用してデータを分析し、インシデントを検出します。効率性を最大限に高めるために、相関付けエンジンは複数のソースからインテリジェンスを取得します。

1. **IoCから：**McAfee Enterprise Security ManagerのCyber Threat Managerを利用して、リモートソースからIoCを取得し、環境内のIoC活動を素早く検証できます。管理者は、STIX/TAXII形式の業界フィード（FS-ISAC）、McAfee Advanced Threat Defense、サードパーティのWeb URLなどのIoCフィードを継続的に利用するよう設定し、このデータをウォッチリスト、アラーム、レポートなどにフィードできます。次に管理者は、リアルタイム監視用の専用ダッシュボードを使用できます。IoC取得ワークフローの一環として、McAfee Enterprise Security ManagerのBackTrace機能により、保管中のネットワークデータやシステムデータ内の最大過去60日間の指標を追跡できます。たとえば、新たに特定されたマルウェアソースと過去に通信していた内部システムを特定できるので、攻撃を再現して封じ込めることができます。McAfee Threat Intelligence Exchangeとの統合により、IoCアーティファクトによって悪質と判断されたファイルにアクセスしたか、このファイルを実行したことがある管理対象エンドポイントも特定できます。
2. **McAfee Global Threat Intelligence（McAfee GTI）から：**McAfee GTIウォッチリストが、SIEMソリューションに自動的にIPアドレス、URL、マルウェアに関するレピュテーション情報を提供します。

相関付けエンジンは、組み込みの相関付けルールに加えて、以下の分析メソッドを使用します。

1. **Intel Securityが提供するコンテンツパックから：**悪質な活動、マルウェア、偵察、不審な活動などの特定の用途向けの相関付けルール、アラーム、ウォッチリスト、ダッシュボードが提供されます。
2. **ベースラインから：**McAfee Enterprise Security Managerによって環境内の正常な状況のベースラインが確立され、このベースラインから外れたものをIoCとして使用できます。たとえば、ユーザーが普段は北米に位置するWebサイトにアクセスする企業で、事業展開していない東欧の国のサイトとの通信が営業時間以外に急増した場合、一部のシステムが侵害され攻撃者と通信している可能性があります。
3. **カスタマイズされたルールから：**Enterprise Security Managerが、企業独自のニーズとリスク許容度に対応するカスタム相関付けルールを作成する機能を提供します。たとえば、システム内で未知のファイルが実行され、1人のユーザーに対して1時間以内に10以上のウイルスが検知されたときにアラートを受信する独自の相関付けルールを記述できます。通常これは、ユーザーの資格情報が侵害され、何者かがシステム内に侵入を試みている証拠です。

これらのセキュリティ情報と強力な分析エンジンを提供するMcAfee Enterprise Security Managerは、相関付けを実行して現在、過去、または将来の攻撃を自動的に検知し、優先的に対処することができます。

- **McAfee Advanced Threat Defenseがゼロデイマルウェアを検知し、ローカル脅威情報を生成。**McAfee Advanced Threat Defenseは、ファイルを分析して悪質であると断定した場合、このマルウェアに一致するIoCのリストを生成します。McAfee Advanced Threat Defenseは、サンドボックスでこのファイルを実行させて動的な分析を行うだけでなく、ファイルのソースコードをアンパックして完全に見直す静的コード分析も実行します。このとき、元のペイロードと、コード内に存在しうるネスト化されたペイロード両方が分析されます。したがってAdvanced Threat Defenseは、このマルウェアと関連する包括的なIoCを生成できます。この情報には、名前、ハッシュ（MD5またはSHA-1）、断定されたファイルの重大度、最初に検知されたシステム、含まれていたメッセージ、ソースおよび宛先システム、ソースURL（該当する場合）などが含まれます。McAfee Advanced Threat Defenseは、業界標準のSTIX（Structured Threat Information eXpression）形式のレポートを生成します。マルウェアの詳細情報がオープン形式で提供されるため、管理者はマルウェアの意図を理解し、McAfee Enterprise Security ManagerのCyber Threat Managerなどの他のセキュリティアプリケーションと結果を共有できます。これらのアプリケーションは分析でこの脅威インテリジェンスを活用します。
- **McAfee Active Responseがエンドポイントの侵害指標をプロアクティブに調査。**McAfee Active Responseによってエンドポイントに対する可視性が継続的に提供されるため、侵害を速やかに特定できます。このソリューションが装備するコレクタは、攻撃イベントの検知時にトリガーされ、監視している攻撃活動のアラートを管理者とシステムに提供します。高度に自動化された機能により、エンドポイント内に無活動で潜んでいる攻撃や攻撃コンポーネントを示すと思われるイベントや変更を監視してキャプチャーできます。
- **McAfee Threat Intelligence Exchangeがセキュリティソリューション間のコラボレーションを実現。**DXLは、新たに検知された脅威情報をセキュリティソリューション間で交換するときに使用されるプロトコルです。McAfee Enterprise Security ManagerはDXLをリスンするので、DXLに新しい情報を送信するあらゆる製品を活用できます。McAfee Threat Intelligence Exchangeが新しい悪質なファイルに関する情報をDXLに公開し、このファイルが他のセキュリティ対策によってもレポートされている場合、McAfee Enterprise Security Managerはこの情報を即座に活用してインシデントを作成できます。DXLをリスンするパートナーのネットワークアクセスコントロールソリューションも、この情報を活用してBYOD（持ち込み）システムを含むシステムをチェックし、ネットワークへのアクセスを許可する前にこの新しい悪質なファイルの存在を把握できます。

オプションの統合

製品	SEIMソリューションのデータソース	McAfee Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee ePolicy Orchestrator®（McAfee ePO™）ソフトウェア	検知の例
McAfee Application Control	√			√	• 未許可のアプリケーションの実行
McAfee Data Loss Prevention	√	√		√	• 機密データの抽出 • 未承認のアプリケーションによる機密データへのアクセス • 未許可のストレージデバイス
McAfee Endpoint Intelligence Agent	√			√	• 異常なアプリケーションからのアウトバウンドネットワーク接続
McAfee Network Security Platform/ McAfee Intrusion Prevention System	√	√	√		• C2（ボットネット）トラフィックの検出 • 悪質なIPアドレスとの通信
McAfee Web Gateway	√	√	√	√	• C2（ボットネット）トラフィックの検出 • 悪質なWebサイトへのアクセス • 未許可のWebサイトへのアクセス
McAfee Database Application Monitor	√			√	• 特権データベースアクセスの検知 • データベースの脅威の検知
McAfee Application Data Monitor	√				• 機密データの転送 • 未承認のアプリケーションの使用
McAfee Database Event Monitor	√				• 機密データベースのデータおよびポリシーの違反 • 正当なチャネルを通じたデータベースデータの損失
McAfee Change Control	√			√	• 未許可のシステム変更
McAfee Host Intrusion Prevention	√			√	• マルウェアの検知 • 異常なファイアウォール活動
McAfee VirusScan® Enterprise software	√	√		√	• マルウェアの検知
McAfee SiteAdvisor® Enterprise	√	√		√	• 未許可のWebサイトへのアクセス • 悪質なWebサイトへのアクセス

表1. 他のIntel Security製品との追加の統合によって、可視性と脅威インテリジェンスがさらに強化されます

ソリューションの効果

McAfee Enterprise Security Managerが中央のロケーションの1つのコンソールでセキュリティの個別の要素を統合し、完全な可視性を提供するため、管理者はセキュリティの全体像を把握し、組織のセキュリティ体制に対する重要な洞察を得ることができます。セキュリティチームは、高度な標的型攻撃を検出するために必要なデータをこれまでより容易に収集できるようになります。不審な事象に遭遇しても、アナリストは数分で必要なデータを取得し、貴重な時間を多く費やさずに攻撃に対応できます。

McAfee Enterprise Security Managerが提供する一元管理されたインテリジェンスによって、管理者は環境内で発生する数百万のイベントから生成されるノイズに対処することができます。このインテリジェンスでは自動的にイベントが解明され、重要なインシデントのみが提示されるので、管理者は重要な兆候を見逃さずに把握でき、アラート疲れに陥ることもありません。

Intel Security製品のこの強力な組み合わせにより、管理者は高度な標的型攻撃に起因する捉えにくく検出が難しいIoCを把握することが可能になります。McAfee Advanced Threat DefenseがIoCリストを生成し、McAfee Threat Intelligence Exchangeがこのリストを配布し、McAfee Enterprise Security ManagerとMcAfee Active Responseが過去と現在、そして今後もこれらのIoCを追跡するため、隠された脅威を検出する能力が飛躍的に高まり、その所要時間も削減できます。

つまりこのソリューションによって、時間を敵に回すのでなく味方にすることができます。これらの製品を組み合わせて使用すれば、管理者は、数日、数週間、あるいは数カ月ではなく、発生直後に攻撃を検出することが可能になります。このIntel Securityソリューションにより、損害が及ぶ前に攻撃を阻止できるチャンスがあるゴールデンアワー（最初の侵害直後の時間）中に高度な標的型攻撃を検出できるようになります。

さらに、セキュリティスタッフを作業から解放して有効活用することが可能になり、インシデントの検知ではなく、インシデントへの対応と修復に注力させることができます。

Intel Securityの高度な標的型攻撃検出ソリューションを使用すれば、環境を継続的に監視してリアルタイムで攻撃を検出することが可能になります。また検出時間を大幅に短縮し、即座に措置を講じて攻撃による損害を制限できます。ローカル脅威インテリジェンスを独自に活用することによって環境内にのみ存在する脅威を検出できるようになり、ゼロデイ攻撃の特定のために外部ソースに依存する必要がなくなります。

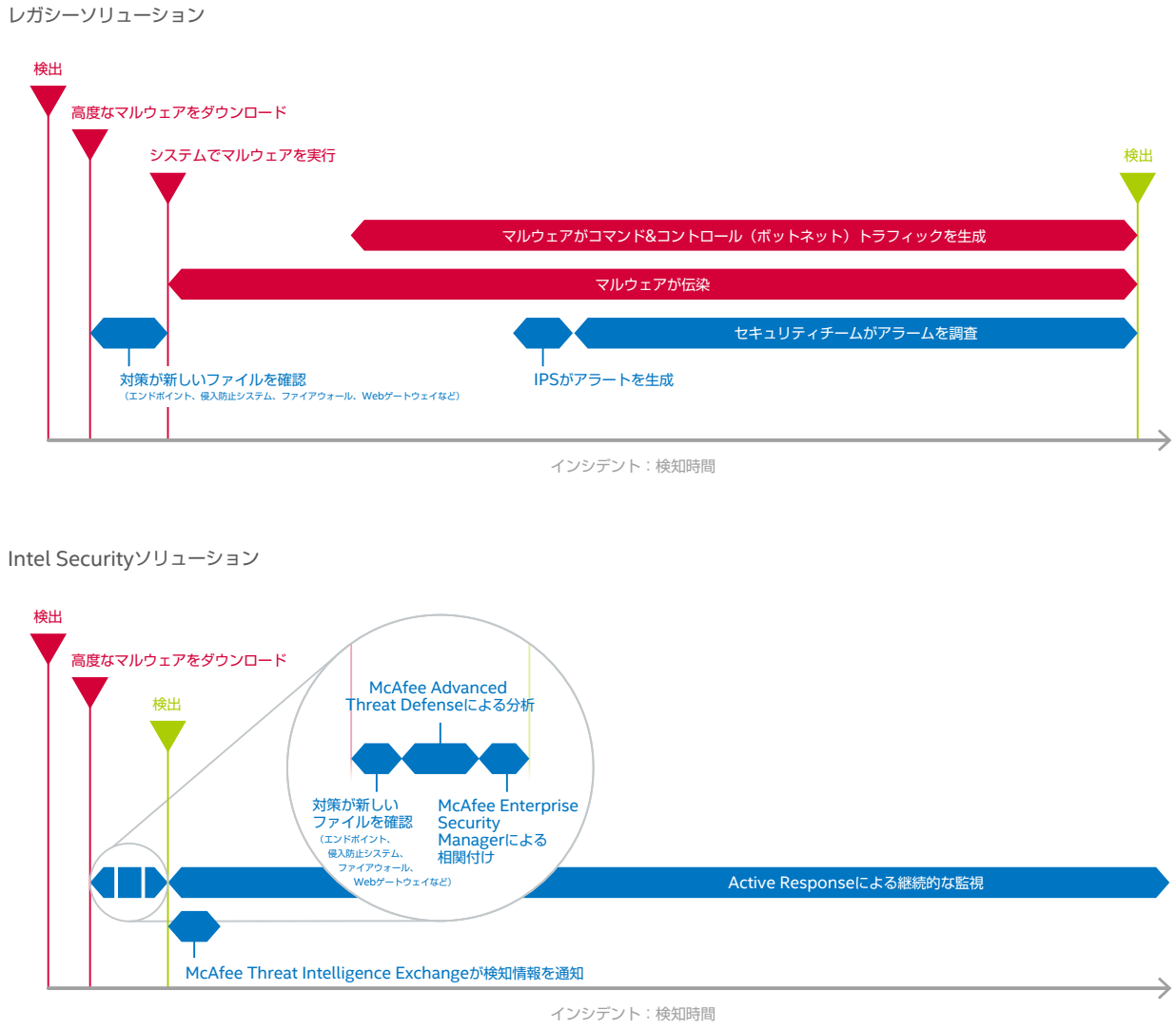

図2. インシデントの検出時間

Q&A

このソリューションはIntel Security製品とのみ連動しますか?

McAfee Enterprise Security Managerは、別のセキュリティソリューションやサードパーティサービスなど、大半のデータソースからイベントを収集できます。ただしIntel Securityでは、McAfee Threat Intelligence Exchangeやその他のIntel Security独自のソリューションが提供する情報を利用してインテリジェンスを強化することをお勧めします。

また、McAfee Security Innovation Allianceを通じて130を超えるテクノロジーパートナーのサポートも受けることができます。パートナーのツールは、Intel SecurityのSecurity Connectedフレームワークで直接利用できます。Security Innovation Allianceにより、お客様はこれまでの投資を活用し、戦略的なツールを導入して必要なときに機能を補完できます。

さらにこのプラットフォームは、STIX/TAXII、IoC、RESTful APIなどのオープンな標準を幅広くサポートしています。Intel Securityの製品では、合理的にオープンな標準を利用できます。

大半のSIEMベンダーはマカフィーと同じ機能を提供できると主張しています。McAfee Enterprise Security Managerの独自のメリットは何ですか?
Intel Securityの製品はSIEMソリューションの域を超えるメリットを提供します。McAfee Enterprise Security Managerはこのソリューションの中心をなしていますが、McAfee Advanced Threat Defense、McAfee Threat Intelligence Exchange/DXL、防御機能の他のコンポーネントと脅威データを即座に交換できる機能、McAfee Active Responseのリアルタイムで IoCを検索できる機能によって、この包括的なソリューションが実現しています。独自のローカル脅威インテリジェンスを生成して共有し、リアルタイムで活用できる機能によって、Intel Securityソリューションは比類のない強力なソリューションになっています。セキュリティ製品の1つによって情報が発見され次第、すべてのセキュリティソリューションが攻撃を検出し、システム全体を即座に強化できるようにするには、この機能が極めて重要です。また、McAfee Enterprise Security ManagerのBackTrace機能が過去に遭遇した指標を探し出すため、かつて特定の攻撃のリスクにさらされたかどうかも把握できます。

独自のヘルプデスクソリューションを使用してアラートとインシデントを管理していますが、Intel Securityのソリューションと連動させることはできますか?
もちろんです。McAfee Enterprise Security Managerは、Remedyなどのサードパーティチケットシステムと統合し、アラートを転送することができます。

MCABP-ATAD-1604-GRP