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：復旧

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 III

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。本書では柔軟な調査と迅速な復旧のために、重度判定と優先順位決定を促進する方法について説明しています。これらの方法を習得することにより、コラボレーションインフラストラクチャ全体にインサイトをすぐ適用できるようなソリューションが確立されます。全体像を把握するためには、3部作の他の2冊、Protect(防御)とDetect(検知)のブループリントをご覧ください。

対応のスピードアップ

状況

どのセキュリティチームも一番恐れているのが、「不正侵入されてしまった」という知らせです。攻撃者が自社ネットワークに侵入していることがわかったら、どうすればよいのでしょうか。被害が発生する前に、攻撃を無効化するにはどうすればよいのでしょうか。いつでも対応して復旧できる態勢が整っていますか。ご存じのように、問題解決に時間がかかるほど、組織が被る被害が大きくなります。どこから手を付ければよいのでしょうか。すぐに「止血する」方法はあるのでしょうか。すぐに対応しなければなりませんが、同時にオーバーリアクションも避けなければなりません。つまり、不要なアクセス停止や本番システムのシャットダウンはしないでください。微妙なバランスが必要です。最初の対応後は、攻撃を調査し、クリーンアップし、環境内に脅威が存在しなくなったことを確認する必要があります。

懸念の拡大

できるだけ早くインシデントに対応することは攻撃を阻止し、大規模な被害を食い止めるためには不可欠なことです。しかし、解決プロセス全体が完了するまでに数週間、または数か月かかることがあります。Ponemon Instituteの2014年のレポートによると、「サイバー攻撃を阻止するのに平均で31日間かかっている[1]」ことがわかりました。インシデントへの対処を難しくしている理由を以下にいくつか挙げます。

- **手動プロセス。**多くのセキュリティチームでは、インシデントへの対応を手作業で行っているため、対応プロセスの遅れによって迅速なインシデント検出が難しくなっています。完全に手作業で対応する場合、対処方法や優先順位に関して、セキュリティチームの専門知識に依存することが多くなります。残念ながら、セキュリティチームのリソースは限定的です。攻撃発生時に発生しがちなインシデント量の増加や複雑化が生じても、セキュリティチームを容易に拡張することはできないのです。場合によっては、チームは1つのインシデントの解決をあきらめて、次のインシデントに取り組まなければならないこともあります。チームが調査やクリーンアップのためのリソースを他の部門から「急きょ確保して増員」することが一般的ですが、これは持続可能なソリューションではなく、解決プロセスに余計な時間がかかってしまいます。

  インシデントへの対応に、御社はどのようなリソースを使用していますか? 該当するものをすべて選択してください。

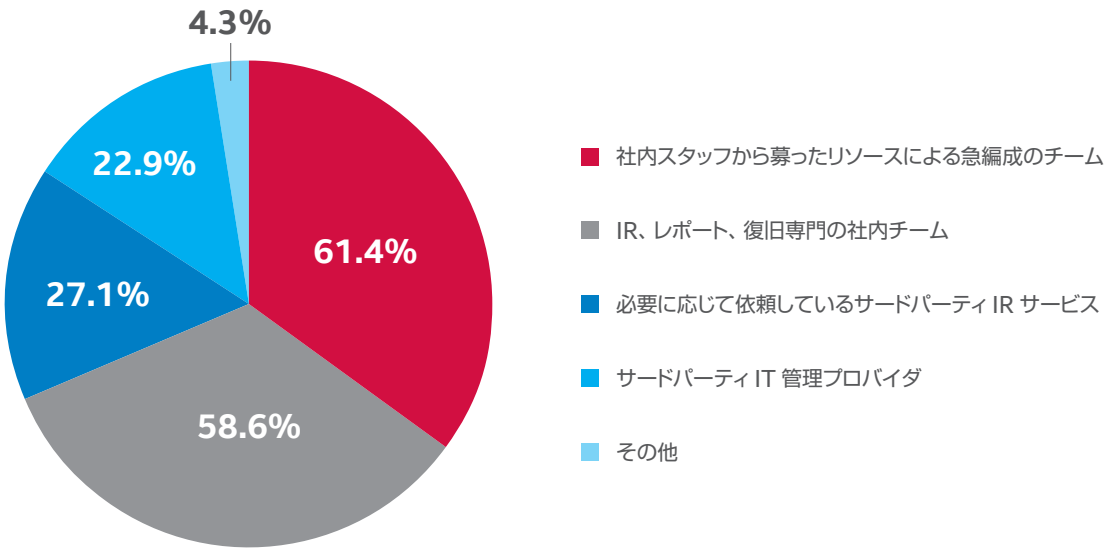

図1. 組織が活用しているIRリソースの種類。出典:*SANSインシデント対応調査、2014年*

- **一元化された復旧ツールの欠如。**サイロ化された運用によって、すぐに対応することが困難になっています。必要な作業を完了するために、複数の部署に協力を求めてコラボレーションしなければならないことがよくあります。たとえば、ネットワークチームに特定のIPアドレスのブロックを依頼する必要があるかもしれません。残念ながら、実際にそうしたアクションを実行するには数時間かかることがあります。

- **サイロ化され、分散されたデータソース。**スタンドアロンセキュリティ製品を使用している場合、調査やフォレンジックに時間がかかります。侵害発生前にログ収集ソリューションを導入していない場合、侵害後に複数のソースから必要なデータを収集し、分析しようとすると非常に時間がかかってしまいます。これによって、何が起きたのか。攻撃者の痕跡は残っているのか。侵入方法は。誰の情報が漏えいしたのか。被害は発生しているのか（データ漏えい、アカウントへの感染など）。被害があった場合はその規模。侵害発生からどの程度時間が経っているのか。誰が感染したのか。どのマシン、どのユーザーが感染したのか。といった重要な質問に答えることができません。
- **迅速な対応と正確な意思決定のバランス。**侵害発生後、一番避けたいのが誤検出です。これによって、インシデント回避プロセスで本番システムを不必要に中断させることになるからです。セキュリティチームは、検疫しようとしているサーバーや、ブロックしようとしているIPアドレスをどうしてもオフラインにする必要があるのかどうかを見極める必要があります。リスクの高い行動をするよりも、しばらく様子を見るというアプローチを選択する場合もあります。しかしこのプロセスによって、解決までの時間が長くなり、リスクが高まります。

ソリューションの説明

Intel Securityでは、組織が攻撃への対応と分析について、可能な限り優先順位を付け、自動化できるような、統合セキュリティフレームワークを導入し、インシデント対応までの時間をできるだけ短縮することを推奨しています。最初の対応後、ソリューションによって対応チームはすぐに調査することができ、できるだけ早期に細かい復旧作業を開始できます。そして最終的にはソリューションが攻撃内容を把握して学習するため、その後のアプローチが迅速になり、次回の攻撃発生時の対応が速くなります。つまり、このフレームワークによってセキュリティチームは次のような対応プロセスに従うことができます。抑制の自動化、迅速な調査、侵害されたシステムをすぐ、確実に復旧、そのインシデントから学習。

1. **迅速な対応のオーケストレーション。**理想的には、標的型攻撃（関連するDetect（検知）ブループリントで説明している）に対してはすぐに対処する必要があります。ウイルス対策ソフトウェアがマルウェアを検出するとすぐにブロック、削除するように、ソリューションが最初の対応をして、攻撃者による環境への侵入を制限、または阻止する必要があります。たとえば、ソリューションが最初の感染者を自動的に隔離し、攻撃者への通信をブロックする、またはリスクのあるシステムには強力なセキュリティポリシーを適用する必要があります。

   当然ながら、ソリューションは最初の感染者、攻撃者に侵害されたIPアドレス、リスクのあるシステムを特定できるだけの十分なインテリジェンスを入手できなければなりません。これによって、長時間の手動分析が不要になります。迅速かつ自動化された対応によって、進行中の攻撃を数秒で阻止できます。確実に自動化するためには、ソリューションは各種のセキュリティ対策と統合し、そしてそれらのセキュリティ対策も相互に統合する必要があります。対処と確実性のバランスが維持されるように、事前定義済みの条件で設定でき、きめ細かく、リスクベースの対応が可能でなければなりません。
2. **迅速な調査。**緊急対処後はインシデントを詳しく調査することができます。調査によって、侵害の規模、発生方法、感染した人を特定できます。

   適切な情報への簡単なアクセスは、迅速かつ詳細な調査には欠かせません。そのため、ソリューションにはデータを簡単に処理し、履歴確認によって何が発生したのかを調べ、根本原因を特定できるような機能が必要です。また、次のような疑問にもすぐ答えられるように詳細なコンテキストも提供できなければなりません。影響があったのは誰か。いつ影響が発生したのか。どのように影響が発生したのか。影響が発生したシステムはビジネス上重要なものなのか。影響を受けたユーザーは幹部など、注目されやすいユーザーなのか。

   さらに、ソリューションは外部の脅威情報などのサードパーティや、サンドボックスなどの社内ソースなど、利用可能なあらゆるソースから関連する脅威インテリジェンスを収集できなければなりません。いずれの場合でも、侵害指標（IoC）、新たに検出した悪意のあるファイルのハッシュ値、悪意のあるIPのリストなどを収集する必要があります。その後、ソリューションは発生した、または発生中のイベントを、このインテリジェンスと照合し、迅速かつ正確な調査を行います。最後に、ソリューションによって得たデータ、コンテキスト、インテリジェンスによって、最も重要なインシデントを優先的に処理できるようにすることで、限られたリソースを適切に活用できます。
3. **侵害されたシステムの復旧。**調査を終え、攻撃について完全に理解したら、復旧プロセスを開始できます。ソリューションは、インシデントの復旧に必要なタスクを実行できるように、十分に一元化された機能を提供する必要があります。コンピュータから数ファイルを削除し、脆弱性のあるソフトウェアにパッチを適用するといった簡単なタスクの場合も、救済不可のシステムにリモートでイメージをリロードするといった複雑なタスクの場合もあります。回復プロセスを進める中で、漏れがないことを確認する必要もあります。そのため、ソリューションでは環境内でプロアクティブにIoCを検索できなければなりません。これにより、脅威の再発を待つのではなく、事前に検索して対処することができます。
4. **発生したインシデントから学習。**攻撃をブロックするたびに、攻撃者に対して攻撃された側の情報が提供されてしまいます。そして攻撃者はその情報を基に、攻撃内容を洗練します。攻撃者に常に対抗するためには、攻撃を受けた側とそのセキュリティインフラストラクチャも発生したインシデントから学ぶ必要があります。ソリューションは攻撃に関して、アクションに結び付く情報を提供する必要があります。これによって、ポリシーを強化し、防御態勢やIT戦略を更新し、この攻撃や将来発生する類似の攻撃をすぐにブロックすることができます。可能であれば、このような情報をITやセキュリティシステムとも共有し、インフラストラクチャに学習させて、適応させる必要があります。

意思決定の要素

アーキテクチャには、次のような要素が影響します。

- 現在、セキュリティ製品やその他の製品からどのようなイベントを収集していますか?
- 社内に専門のインシデント対応チームや、マルウェアおよび攻撃のフォレンジックを担当している専門スタッフがいますか?
- 各セキュリティソリューションを担当しているチームは、異なる部署にサイロ化されていますか?

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

Intel® Securityソリューションは、推奨しているインシデント対応プロセスの各ステップに対応したテクノロジーを提供しています。これにはMcAfee® Enterprise Security Manager、McAfee Threat Intelligence Exchange、McAfee Active Response、McAfee ePolicy Orchestrator®（McAfee ePO™）ソフトウェア、McAfee ePO Deep Command、McAfee Advanced Threat Defenseが含まれています。これらのソリューションの大半はプロセスとツールを連携し、複数の段階（標的型攻撃を阻止するためのProtect（防御）とDetect（検知）段階を含む）をサポートし、各種タスクに使用できます。たとえば攻撃され、復旧不可能と判断したシステムにイメージをリロードするためのMcAfee ePO Deep Commandのように、非常に特殊な要件に対応するためのソリューションもいくつかあります。

図2. 推奨されるインシデント処理ワークフローに対応したIntel Securityソリューション。

1. **迅速な対応のオーケストレーション。** Intel Securityソリューションは、人が直接介入しなくても攻撃による影響を最小化するように設計されています。Security Connectedと呼ばれるセキュリティフレームワークによって、最初の抑止を自動的に行うことができます。Security Connectedフレームワークによって、感染したシステムの検疫や、新たに発見した悪意のあるドメイン、IP、URLのブラックリストへの追加といった主要な抑止作業を自動的に行うことができます。Security Connectedフレームワークでは、ゼロデイマルウェアにも自動的に対応することができます。このような機能を備えた2つの主な製品が、セキュリティ情報とイベント管理（SIEM）プラットフォームであるMcAfee Enterprise Security Managerと、McAfee Threat Intelligence Exchangeです。

- **McAfee Enterprise Security Managerによって、インシデントへの対応を一元化および自動化。** McAfee Enterprise Security Managerは、McAfee ePOソフトウェア、McAfee Network Security Platform（McAfeeの侵入検知システム）、McAfee Threat Intelligence Exchangeなど、他のセキュリティ製品に統合し、必要なアクションに結び付けます。McAfee Enterprise Security ManagerはMcAfee Advanced Threat DefenseからのIoCなど、複数のソースからデータを収集します。また、受信したデータの分析に基づき、他の製品に復旧のためのアクションを指示することもできます。

  たとえばEnterprise Security Managerがインシデントを検出し、侵害されたエンドポイントがネットワーク上で悪意のあるトラフィックを送信していることが判明した場合、McAfee ePOソフトウェアにMcAfee Host Intrusion Preventionポリシーの適用を指示して、エンドポイントの検疫を行わせることができます。ポリシーは非常にきめ細かいため、エンドポイントにMcAfee ePOサーバーとだけ通信させ、システムのリモートコントロールは維持しながら、エンドポイントへの被害が拡大しないようにすることができます。

  あるいは、Enterprise Security Managerが悪意のあるIPアドレスを検出し、ネットワーク上のシステムがそのアドレスと通信している場合、そのIPアドレスへの通信をブロックするようにIntrusion Prevention Systemに指示することもできます。

  McAfee Enterprise Security Managerには多くのIntel Securityやサードパーティテクノロジーおよびデータソースへの接続機能が内蔵されていますが、オープンインターフェイスも提供しているので、サードパーティの他のテクノロジーを使用してオーケストレーションを行うことができます。トリガーに対してカスタムスクリプトを実行するように、McAfee Enterprise Security Managerを構成しておくことができます。Scripting Host上でサポートされている任意のスクリプト言語でスクリプトを作成し、指定されたScripting Host上でスクリプトを実行、またはSSHを使用して実行することもできます。

- **McAfee® Threat Intelligence Exchangeは新しい脅威からプロアクティブに防御。**高度な標的型攻撃の被害に遭った場合、攻撃者はゼロデイマルウェアを使用してシステムに侵入している可能性があります。McAfee Threat Intelligence Exchangeは、ゼロデイ脅威に対して自動的に対応できます。環境内で新たに悪意のあるファイルが検出された場合、そのファイルのレピュテーションを悪意のあるものとして設定し、他のホストでのファイル実行と攻撃能力をブロックし、Intel Securityやパートナーからのネットワークやコンテンツ制御によってブロックを拡大します。悪意のあるファイルは最初の被害者から消去することもできます。

  McAfee Threat Intelligence ExchangeをMcAfee Endpoint Protection、McAfee Advanced Threat Defense、その他のIntel Securityおよびパートナー製品に統合することで、このような介入作業が自動的に行われます。必要であれば、そのファイルに手動でレピュテーションを適用することができます。環境内で何を許可/ブロックするのかをより詳細に設定し、リスク感度と整合させるため、特定のファイルや証明書に対するデフォルトレピュテーションを無効化することができます。これにより、McAfee Threat Intelligence Exchangeはこの情報をData Exchange Layer（DXL）から、環境内に導入されているThreat Intelligence Exchange対応のあらゆる対策ソリューション（ゲートウェイを含む）に伝えます。プロセス全体は1秒以内で実行されます。新たに検出した脅威に対するこのような自動フィードバックループにより、Threat Intelligence Exchangeに対応したすべての導入済みセキュリティ製品が新たな脅威にすぐに対応できます。

2. **迅速な調査。**最初に必要な対応をして攻撃を阻止したら、次にインシデントを詳細に調査して、潜在的な侵害の規模、範囲、影響を把握する必要があります。McAfee Enterprise Security Managerは、このような分析の一部を自動化することで、調査をスピードアップしてくれます。McAfee Active Responseによって環境内で侵害の痕跡を検索し、McAfee Threat Intelligence Exchangeによって侵害をたどるためのユニークでパワフルな情報を入手できます。

- **McAfee Enterprise Security Managerによる分析と調査プロセスのスピードアップ。**分析プロセスの一部を自動化し、必要な情報を提供することで、McAfee Enterprise Security Managerはインシデント調査に必要な時間を短縮します。インシデントのドリルダウン、イベントの詳細入手、データのピボット処理、履歴分析といった機能により、インシデント自体と関連する周辺イベントにすぐアクセスできます。数回クリックするだけで、一連のイベントを再現することができます。さらに、McAfee Enterprise Security Managerではシステムの地理位置情報や重要性、インシデントに関与したユーザーなど、コンテキストデータを追加することもできます。コンテキストが増えることで、調査担当者は攻撃の規模や範囲を正確に把握できるようになります。

  さらに、McAfee Enterprise Security ManagerのBackTrace機能によって、最大60日間の履歴を確認できるので、過去に発生したIoCを探すことができます。たとえば、新たに検出されたマルウェアソースと通信したことがある社内システムを探して、攻撃の再現に利用することができます。サードパーティから新しいIoCを受信した場合、またはMcAfee Advanced Threat Defenseとの統合で新しいIoCを入手した場合は、非常に便利な機能です。BackTraceはこのようなIoCを取り込み、過去にこの種の攻撃の痕跡がないか知らせてくれます。

- **McAfee Active Responseによるリアルタイムの調査。**McAfee Active Responseを使用すると、侵害指標など、すべてのエンドポイントに関する特定の属性をリアルタイムに検索できます。この種の属性にはシステムに注入されたファイル、レジストリキー、メモリ内で実行しているプロセスが含まれます。Active Responseスキャンの実行後は、攻撃コンポーネントが環境内に休眠状態で潜んでいる心配がなくなります。休眠コンポーネントとはダウンロード後、まだ実行されていないものを指し、実行前は検知がほぼ不可能とされているものです。McAfee Active Responseはこの種のコンポーネントを検出できるので、システム内のすべての侵害アーチファクトを確実に検出できます。

- **McAfee Threat Intelligence Exchangeによって、影響を受けたシステムと「最初の感染者」を特定。**McAfee Threat Intelligence Exchangeは、環境内で最初に未知の、または悪意のあるファイルが実行されたときに、その場所と時間を通知することで、そもそも侵害がどのように発生したのかという貴重な情報を提供します。McAfee Threat Intelligence Exchangeは、そのファイルが実行された他の場所とその時間、世界中でそのファイルが検出されているかどうか、自社環境だけを標的として特別に作られたものかどうか、という調査のための貴重な質問にも答えることができます。

3. **侵害されたシステムの復旧。**攻撃について完全に理解したので、次に復旧プロセスを開始できます。McAfee ePOソフトウェアは、ポリシーとエンドポイント管理を統合することでこのプロセスを簡単にします。McAfee ePOコンソールから、組織全体のクリーンアップを開始することができます。

- **McAfee ePOソフトウェアによってエンドポイント復旧を一元化。**McAfee ePOソフトウェアは、マカフィーのエンドポイントセキュリティ製品と多くのマカフィーセキュリティパートナーソリューションが使用する、一元的なポリシー/管理プラットフォームです。インシデント対応でこのソフトウェアを使用することで、管理者やセキュリティチームはエンドポイントをリモートから一元制御できます。この作業は手動、自動いずれでも実行でき、McAfee Enterprise Security Manager、ウイルス対策ソフトウェア、McAfee Host Intrusion Prevention Systemなど、他のセキュリティ対策と組み合わせることで、より広範な自動化を推進することができます。特定の統合された管理ポイントを提供するだけでなく、McAfee ePOソフトウェアは調査時に貴重な情報として、攻撃中にログインしたユーザーなど、エンドポイントに関するコンテキストも収集することにより、McAfee Enterprise Security Managerにフォレンジックデータを提供します。

- **McAfee Threat Intelligence Exchangeは組織全体のクリーンアップを数秒で実行。**悪意のあるファイルや自社のリスクレベル判定で疑わしいと見なされたファイルを特定したら、McAfee Threat Intelligence Exchangeを使用して組織全体でそのファイルのクリーンアップを行うことができます。McAfee Threat Intelligence Exchangeを使用することで、ファイルの根絶を決定した瞬間に、メモリから悪意のあるファイルを消去し、システムから削除することができます。たったワンクリックでファイルのレピュテーションを変更するだけでよいのです。ゼロデイマルウェアを検出した場合、McAfee Threat Intelligence Exchangeでそのファイルに既知の悪意のあるファイルとしてフラグを立てるだけで、エンドポイントのクリーンアップが行われます。

- **McAfee ePO Deep Commandによって、リモートからシステムにイメージをリロード。**場合によっては、システムのクリーンアップよりも簡単な場合や、侵害によってMaster Boot Recordが破損し、システムが機能しなくなった場合など、セキュリティチームからシステムにイメージをリロードするよう勧められる場合があります。システムが離れた場所にあって、ITサポートが物理的に駆けつけられない場合は、マシンに物理的にイメージをリロードすることは困難です。しかしIntel® vPro™ Active Management Technology（Intel AMT）によって、McAfee ePO Deep Commandはオペレーティングシステムより上のレベルでエンドポイントとの通信を可能にし、ブートすらできないシステムへのセキュアリモートアクセスを提供します。その結果、離れた場所で侵害されたクライアントにイメージをリロードすることができます。

- **McAfee Active Responseによって、検出したIoCに対してアクションを実行。**McAfee Active Responseでは、調査に使用するリアルタイムのエンドポイント検索だけでなく、探している、または監視している指標を検出すると、プロセスの消去やファイルの削除といったアクションを、手動または自動で行うことができます。McAfee Active Responseではカスタムスクリプトをインポートできるので、環境内でIoCを検出した場合の対応をカスタマイズできます。
- **McAfee Enterprise Security Managerによって、サイロ化された製品を網羅してアクションを実行。**前述のように、McAfee Enterprise Security Managerは他のセキュリティ製品に統合して、アクションに結び付けることができます。調査によって徹底的な対策の必要性を確認できるため、必要なタイミングで、必要なレベルまで、復旧のためのアクションをオーケストレーションすることができます。これにより、コンソールを切り替えなくても適切なアクションを実施することができます。

4. **発生したインシデントから学習。**インシデントを復旧したら、次は教訓を基にプロアクティブに環境を防御し、将来類似のタイプの攻撃が発生した場合に、検出できるようにします。McAfee Advanced Threat Defense、McAfee Enterprise Security Manager、McAfee Active Responseを使用すると、新しい知識を活用できます。

- **McAfee Advanced Threat Defenseによって、ローカルな脅威インテリジェンスを生成。**動的コード分析（サンドボックス）と静的コード分析の両方の機能により、McAfee Advanced Threat Defenseは分析対象のマルウェアに関連するIoCの完全なリストを、独特の方法で生成することができます。この情報には感染したファイルの名前、ハッシュ（MD5またはSHA-1）、重度、最初に発見したシステム、一緒に送信されたメッセージ、送信元と送信先のシステム、そして該当する場合はソースURLが含まれます。これによって調査のための貴重な情報だけでなく、攻撃から学習するまれな機会が得られます。McAfee Enterprise Security ManagerやMcAfee Threat Intelligence Exchangeなどの他のセキュリティソリューションは、McAfee Advanced Threat Defenseが生成した情報から学習し、対応時に攻撃に関する知識を増やすことができます。こうして対抗手段を強化することで、将来的に類似の攻撃をブロックできるようになります。これは非常に重要な機能です。このマルウェアが組織を標的としてカスタマイズされている場合は、他の人が分析することはないので、特に重要です。
- **McAfee Enterprise Security Managerによって、将来的な攻撃を常に監視。**McAfee Enterprise Security ManagerはIoCに基づき、攻撃が発生したかどうかを判定できますが、この機能を使用して、McAfee Enterprise Security Managerにこの指標を将来監視させることもできます。McAfee Enterprise Security ManagerはIoCを基に関連付けルールを自動的に作成し、将来、このIoCと一致する攻撃が発生した場合に、アクションを求めるアラートを発することができます。さらに、McAfee Enterprise Security Managerはウォッチリストを使用して、過去の攻撃に関与した可能性がある特定のユーザーグループ、IPアドレス、その他の資産を注意深く監視することができます。新しいイベントがウォッチリストと一致する場合、システムは自動的にアクションを実行することも、管理者がすぐ確認、対応できるように、イベントをエレベーションすることもできます。
- **McAfee Active Responseによって、将来的な攻撃を継続的に監視。**McAfee Active Responseによって、セキュリティチームは、新しいファイルの作成、メモリ内で実行しているプロセス、レジストリキーの作成や変更、ロードしているドライバなど、エンドポイント上で発生している各種アクティビティを常に監視することができます。トリガーとコレクタの使用により、McAfee Active Responseはシステムで攻撃の動きなど、監視対象行為が発生した場合、監視しているパラメータをすぐにアラートとして通知できるという特長があります。たとえば、攻撃によってレジストリキーが変更された場合、または対象システム上に特定のファイルが作成された場合、レジストリキーの作成直後、またはそのファイルが別なシステムに保存された直後に、McAfee Active Responseがアラートで通知してくれます。McAfee Active Responseのトリガーによって、重要なイベントを現在だけでなく、将来に渡って継続的に監視することができます。
- **McAfee Threat Intelligence Exchangeによって、リアルタイムで学習内容を共有。**McAfee Threat Intelligence Exchangeにはトランスポートメカニズムがあり、他のセキュリティ製品で学習した内容を、Data Exchange Layer（DXL）と呼ばれる通信レイヤーで共有できます。ファイルや証明書のレピュテーション、およびマルウェア情報などを共有できます。McAfee Threat Intelligence Exchange、McAfee Web Gateway、McAfee Intrusion Prevention System、McAfee Advanced Threat Defense、McAfee Endpoint Protectionをすべて DXLで接続することで、統合済みのパートナー製品も使用可能になります。DXLはオープンな通信標準を使用して、任意のセキュリティ製品にDXL上で共有している情報を提供し、活用できるようにします。

オプションの統合

- **McAfee Network Security Platformによって悪意のあるトラフィックを阻止。**攻撃を検出すると、McAfee Intrusion Prevention Systemがその場で対処方法を提示して、対応に要する時間を短縮してくれます。たとえば、McAfee Enterprise Security Managerが感染した他のシステムが通信しているIPアドレスを検出した場合、Intrusion Prevention SystemにそのIPアドレスをブロックするように指示することができます。McAfee Enterprise Security ManagerはIntrusion Prevention Systemに対して、攻撃検出前は監視しか行っていなかったIntrusion Prevention Systemシグネチャをブロックするよう指示することもできます。
- **McAfee Host Intrusion Prevention Systemによって感染したエンドポイントを検疫し、そのエンドポイントとの間で悪意のあるトラフィックの送受信を阻止。**McAfee Host Intrusion Prevention Systemは、攻撃の検出時にその場で対処方法を提示して、攻撃にすぐ対応できるようにします。ネットワーク用のIntrusion Prevention Systemと同様に、McAfee Enterprise Security Managerは、Host Intrusion Prevention Systemに対してネットワーク上の感染したエンドポイントとの通信を中断またはブロックするか、自身が感染している場合はホストを検疫するか、のいずれかを指示することができます。

ソリューションの効果

侵害を検出したら、その後は1秒も無駄にはできません。対応が遅れるほど、被害が拡大します。マカフィーのソリューションを使用すれば、インシデントへの対応に要する時間を最小限にすることができます。自動的にアクションを実行し、検出から数秒で重要な最初の対応を行うことで、できるだけ早期に被害を食い止めます。このソリューションは次に検出から完全な復旧までに必要な作業を行うため、最初にセキュリティ対応チームが侵害の技術面だけでなく、範囲や規模についてもすぐ、正確に理解できるようにします。Intel Securityの調査では、これがインシデント対応で最も時間のかかる作業だということがわかっています。[2]

調査が終わると、Intel Securityソリューションは効率よく確実かつ完全に復旧するためのツールを提供し、復旧に要する時間を数週間から数時間に短縮します。これだけにとどまらず、このソリューションはインシデントから学習することで、防御機能を高め、将来の攻撃に対する防御と対応をさらにスピードアップできるようにします。このように統合、最適化されたシステムにより、高度な標的型攻撃にも大きな効果が発揮できます。

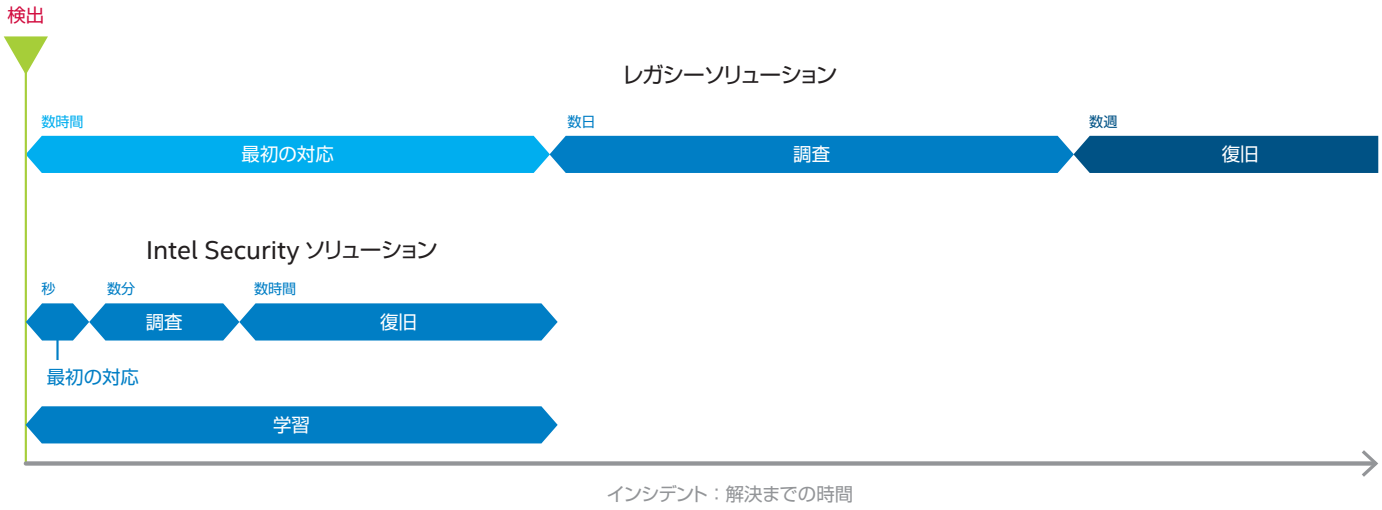

図3. セキュリティインシデントの解決に要する時間。

Q&A

フォレンジックツールはもう導入済みなので、Intel Securityソリューションの必要性がわからない。

既存のフォレンジックツールをIntel Securityの「correct（復旧）」ソリューションに入れ替える必要はありません。検知から復旧までの時間を短縮するためのものです。攻撃に関する調査は全体的なプロセスの一部に過ぎません。マカフィーのソリューションは、より詳細な調査や、訴訟が発生した場合でも適切な対応ができるように、どのシステムからダンプを入手すべきかをすぐに通知することで、フォレンジックをスピードアップします。

社内のエンドポイントチームとネットワークチームがあまり連携していない。セキュリティ運用チームともあまり連携しておらず、入手したデータを共有したがらない。

まさにこのような理由でSecurity Connectedプラットフォームが必要なのです。McAfee Threat Intelligence ExchangeとDXLによってテクノロジーを統合することにより、その製品が環境内のどこにあるのかに関係なく、そして管理者が利用できるコラボレーションツールにも関係なく、セキュリティに関係するすべての製品間で、確実に通信とコラボレーションが行えるようにします。

独自の特定アーキテクチャに縛られたくない。

Intel Security製品は、130以上のサードパーティ製品に統合されており、STIX/TAXII、IoC、RESTful APIを含む多種多様なオープンスタンダードにも対応しています。マカフィーの製品では妥当と判断した場合に、オープンスタンダードをサポートしています。たとえばDXLフレームワークは、通信に関するオープンスタンダードを使用しています。

1.『2014 Global Report on the Cost of Cyber Crime（サイバー犯罪のコストに関するグローバルレポート、2014年）』、Ponemon Institute、2014年10月
2. Intel SecurityとESGによる調査と分析、2015年4月、『Tackling Attack Detection and Incident Response（攻撃の検知とインシデントへの対応）』

MCABP-ATAC-1604-GRP