McAfee MVISION Insights

検出と対応の拡大 (XDR) セキュリティ機能を持つ初めてのエンドポイント保護ソリューションで、攻撃者の一歩先を行く

サイバー攻撃の進化とスピードは、組織にとって絶えず続く脅威となり、重圧となっています。企業はセキュリティ専門家の不足をセキュリティ予算の拡大で補っていますが、ツール、戦略、テクニックを次々と変える現代の攻撃に対処しきれていません。現在の対策は、人と手作業での対応を必要とする、サイロ化したインテリジェンスに頼っています。これは差し迫った脅威には有効かもしれませんが、サイバー攻撃が増大し多様化する中、セキュリティ チームの対応は後手後手になっています。脅威インテリジェンス プラットフォーム (TIP) から得られる大規模なデータレイクを活用するには手作業での統合やアナリストの作業が必要で、実践力や修復機能が限定されます。さらに、脆弱性管理によって既存の脆弱性やその度合いについての助言は得られますが、組織のセキュリティ ポスチャが現実の脅威をどう防御できるかといった情報の提供は十分ではありません。

こうした問題は、プロアクティブなアクションを可能にするリアルタイム インテリジェンスを提供する McAfee® MVISION Insights で解決できます。AI 及び専門家の知見を使って抽出、分析された包括的なインテリジェンスで、危険性が高い脅威やキャンペーンを優先順位付けできます。MVISION Insights は、脅威が組織全体に与える影響を予測して、セキュリティ体制を最適化するためになすべきことを具体的に示します。

主な特長

- **10 億個のセンサーから収集するリスク インテリジェンス：**信頼できるソースを使って、外部脅威をプロアクティブに識別します。脅威プロジェクトを業界、地域、攻撃者、セキュリティ ポスチャに基づいて優先順位付けします。
- **攻撃を受ける前に脅威キャンペーンを識別し、1 つのコンソールから自社のリスクをレベル分けする：**脅威に関する実践的なインテリジェンスを取得し、組織のエンドポイント セキュリティ ポスチャの有効性を把握します（推奨修復策を含む）。
- **検出と解決にかかる平均時間を短縮：**ワークフローを効率化して保護策を強化します。現行のエンドポイント / クラウド セキュリティ ポスチャを評価して、必要となる実践的な改善策を提示し、対応時間を数か月から数時間に短縮します。

McAfee へアクセス

組織のセキュリティを変革して、よりプロアクティブに

MVISION Insights は、McAfee® 管理プラットフォームに組み込まれた機能です。リスクと脅威オペレーションを連携させて効率化し、リソースの投入を抑えながら、予防的に防御策に改善を加え、対応時間も短縮します。10 億個ものセンサーを用いて収集し高度な脅威研究者が精査したリスク インテリジェンスから、対策の優先順位をつけるために必要となる情報を提供します。検出、修復、予防的な対応、対応時間の短縮、大幅なリスク低減のすべてを 1 つのコンソールから実現できます。

リアクティブな事後対応型のサイバー対策は重要な役割を果たしますが、防火活動はせずに火事が起こった後に駆けつけて消火活動を行うようなものです。一方、攻撃者は次世代ツールを使って既存の防御策を打破しようとキャンペーンを画策し、リアクティブなセキュリティ製品の突破方法を試しながらテクニックを向上させています。このため組織は、攻撃の前後を含む攻撃のサイクル全体に対処する必要があります。

攻撃ライフサイクル全体をカバー

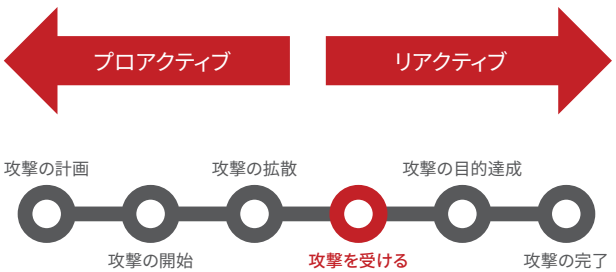

図 1. 典型的な攻撃のサイクル

インテリジェンスと実践的な情報があれば、危険性が高い脅威に対して最善のサイバーセキュリティ対策を構築して、自信を持って対処することができます。これを実現する McAfee MVISION Insights のしくみは次のようになっています。

- **目に見えなかったグローバル脅威を自動的に識別：** MVISION Insights は、10 億個以上のセンサーから集めた大量のセキュリティ インテリジェンスと、人と機械の連携を使って最適化された脅威分析を活用します。機械学習があれば、可視化と処理が不十分でアナリストでは見つけられないような脅威でも検出できます。攻撃者の知恵や工夫に打ち勝つには機械の処理能力に加えてアナリストの直感と専門性も必要です。
- **状況をより詳しく認識し、重要な点にフォーカスします：** 攻撃を受ける前に、自社の防御策の状況を正確に把握できます。MVISION Insights では予測されるローカルの脅威やグローバルな脅威をプロアクティブに追跡して優先順位を付けます。
- **機械学習分析：** エンドポイントやクラウドに関係する包括的セキュリティ ポスチャの実効性を把握し、迅速かつ容易に実装できる予防的な防御策を提示します。

MVISION Insights は、エンドポイントとそれ以外のリスクに関する質問にお答えします。

- 現在リスクにさらされているか？危険の度合いはどの程度か？
- 組織を襲う可能性のある攻撃をどのように優先順位付けするか？その把握方法は？調査プロセスは？
- 今後攻撃を受ける可能性がある脅威をどのように把握するか？
- TIP データベース内のすべての攻撃をどのように優先順位付けするか？
- 同じような企業を襲った脅威についてどのように把握するか？
- 業界や地域でこの脅威はどの程度拡散しているか？
- 自組織を狙う特定の攻撃者がいるか？
- この脅威に対して、現行のセキュリティ ポスチャは十分な耐性があるか？
- 脅威ランドスケープ全体に対抗できる自信はあるか？その根拠は？

MVISION Insights ダッシュボードでプロアクティブなセキュリティを実現

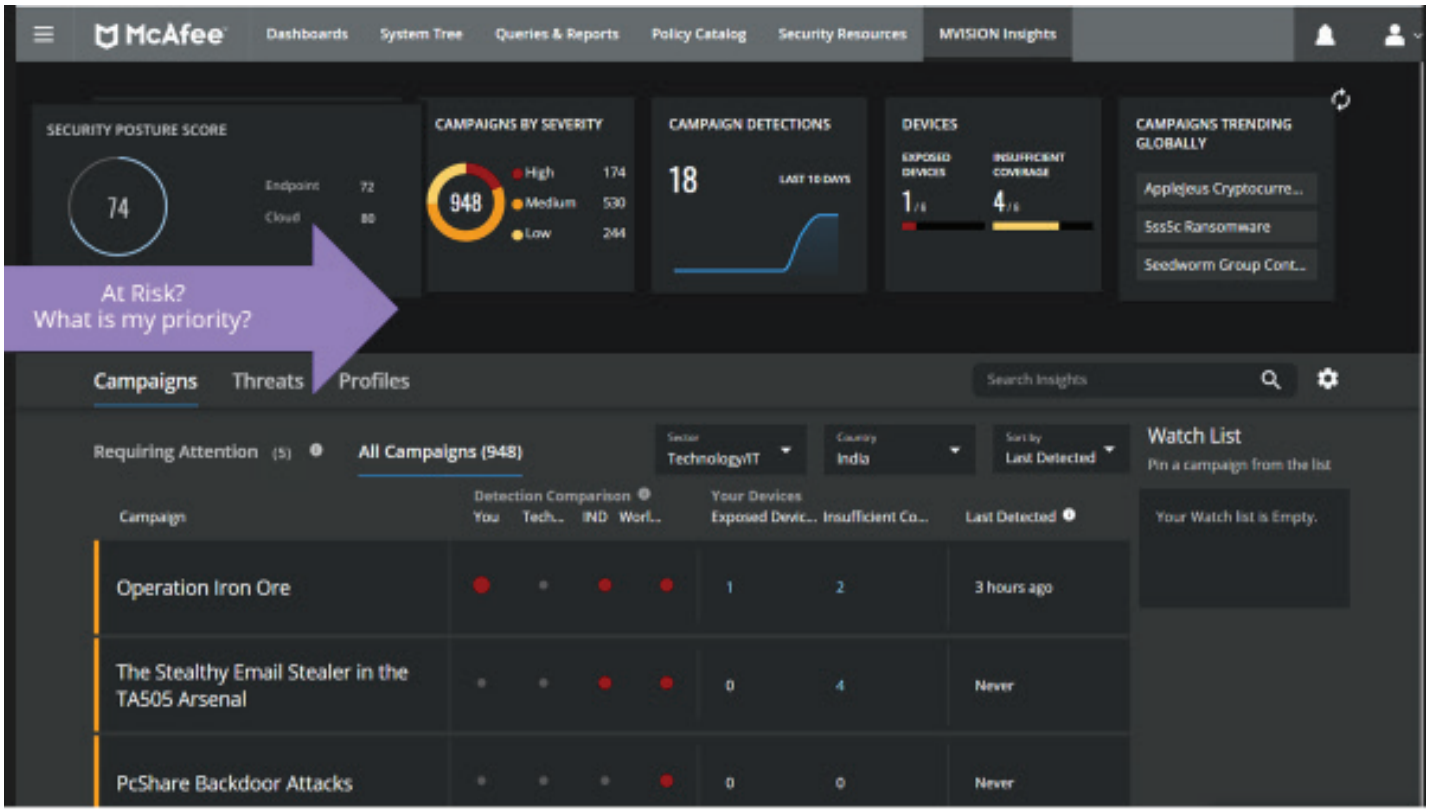

図2.MVISION Insights ダッシュボード

包括的セキュリティ ポスチャで高度化

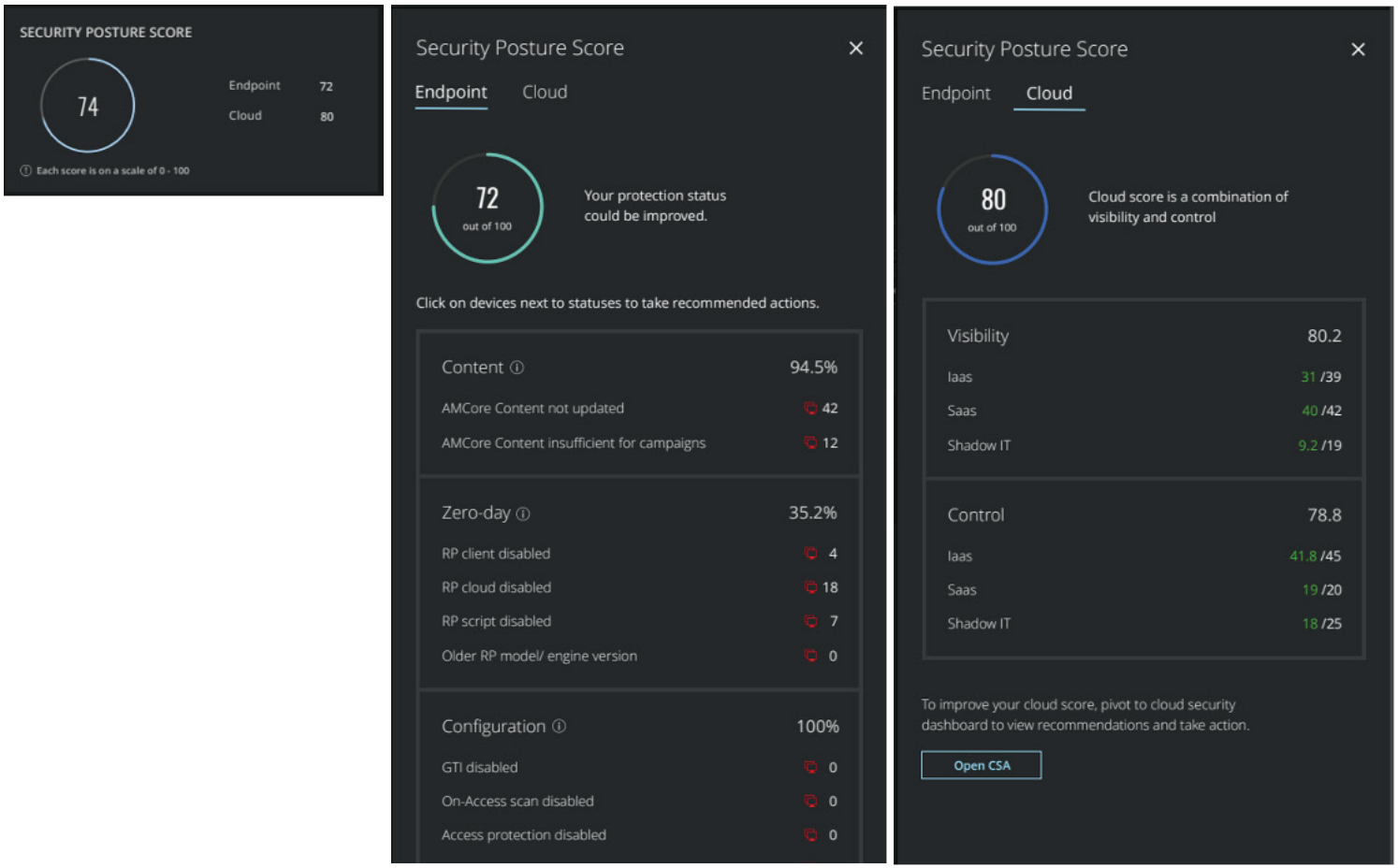

図3.統合的かつ実用的なセキュリティ ポスチャ スコアの概要。

実用的なリスク評価

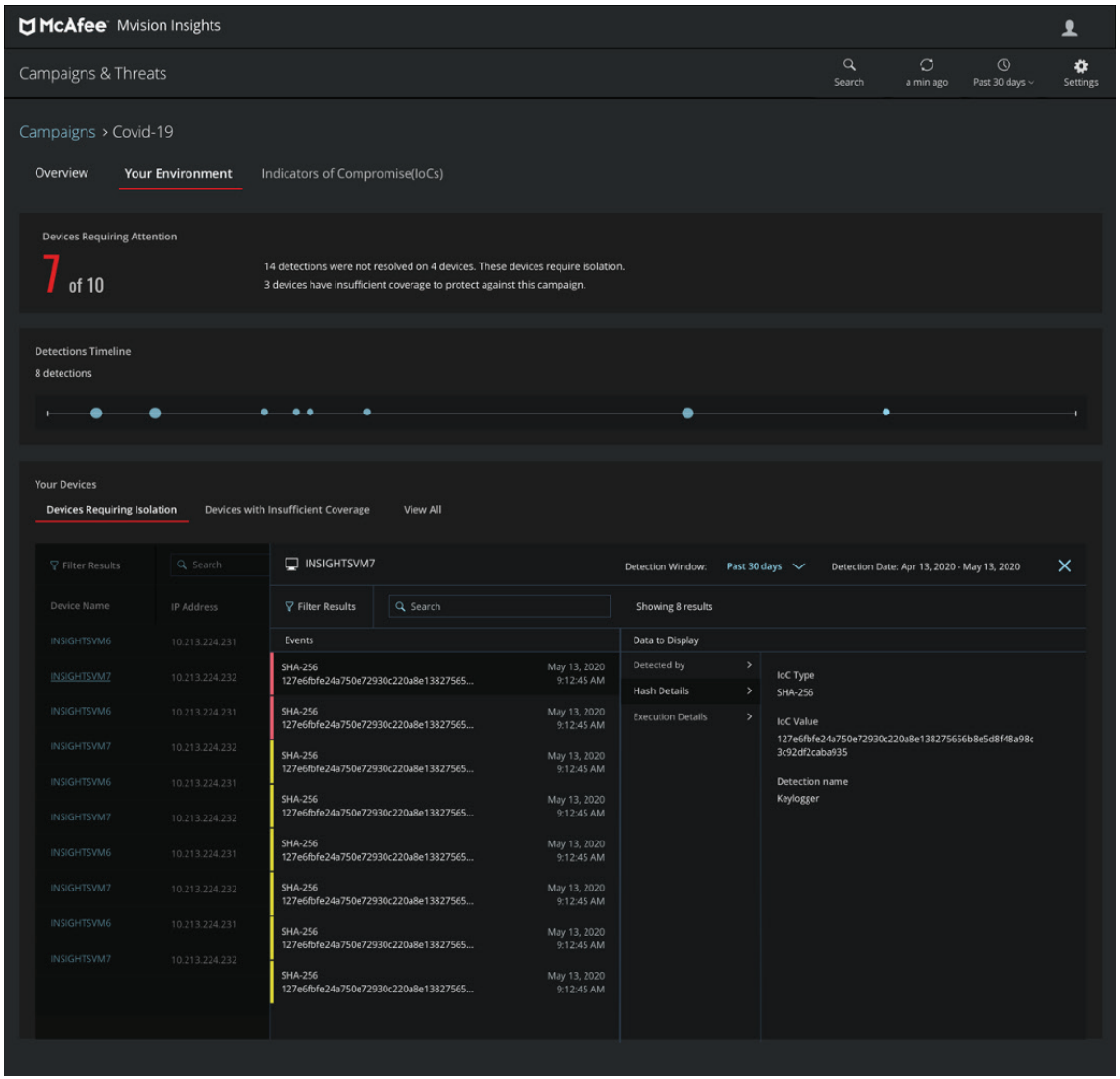

図4.組織の環境内に存在する、注意を要する問題を確認することで、脅威に対してプロアクティブに対応できるようになります。

検出と対応にかかる時間を大幅に短縮

MVISION Insights は、規範的ガイダンスと自動アクションを提供して、それぞれの環境に最適なプロアクティブな対応をサポートします。自動化によって外部脅威の自動分析や比較が可能になり、攻撃を受ける前にプロアクティブに防御できるようになるので、外部攻撃対策の効果を高めることができます。

- **検出から解決までの時間を数か月から数分に短縮：**人と機械の連携 (ディープ ラーニングや機械学習) や高度な分析機能を拡張し、膨大なデータから情報を選り分けて実践的なインテリジェンスを提示します。高度な検出機能により、レスポンスタイムの短縮やリスクの大幅な削減を実現できます。
- **脅威指標の質を向上：**高度な分析で検出精度を向上させ、アラートの精度を高めます。MVISION Insights の脅威分析では、McAfee® MVISION EDR に簡単に切り替えて、侵害の痕跡 (IoC) などのコンテキスト情報を検索でき、調査サイクルを短縮できます。キャンペーンの背後にある攻撃者/犯罪シンジケートに関する重要なコンテキスト (関連するツール、共通脆弱性識別子 (CVE)、標準的な戦術/サブテクニック、関連する IoC、シンジケートの情報) を共有します。
- **脅威に優先順位を付け、実践的かつ理解しやすい形で提示：**包括的な統合セキュリティ ポスチャ (エンドポイント/クラウド評価を含む) では組織の環境にとって重要な点にフォーカスできるようになります。分析され優先順位付けされたインテリジェンスと知見に基づいたレスポンスガイドが提供されるので、経験の少ないアナリストでも対応可能です。統合されたコンソールから、設定を変更し、感染したデバイスを分離し、ポリシーを更新し、エンドポイントでの検出と対応 (EDR) に切り替えるなど、迅速かつ容易に対策を講じることができます。

SOC のリソースを強化

セキュリティチームは大量のインテリジェンスをふるいにかけなければならず、疲弊しています。リソースや時間には限界があり、これが脅威の分析や防御策の足かせとなっています。人と機械の連携を用いれば、アナリストのスキル レベルにかかわらず分析能力を強化して、膨大なデータを処理し、実践的なインテリジェンスとして提示することができます。MVISION Insights はスキルギャップを埋め SOC の生産性を向上させます。さらにセキュリティチームはより高度な情報を手に、的確な判断を下すことができるようになります。

- セキュリティ チームは、データ インテリジェンスから得られる専門家の知見を用いて、組織の防御策をカスタマイズし、強化することができます。人員の増強や高い専門性に頼る

必要はありません。MVISION Insights は、より目的に即した情報を MVISION EDR に提供します。これにより調査サイクルが短縮され、調査に必要となる知識やリソースが得られることから、アナリストはインシデントのリスクや根本原因を、迅速かつ効果的に検証できるようになります。

- 最高セキュリティ担当者 (CSO) は人員や製品を最大限に活かすことができるようになります。セキュリティ アナリストは煩雑な業務から解放され、経験の浅いチームメンバーでもより効果的に仕事ができるようになります。セキュリティ管理にかかる時間は短縮され、ワークフローは効率化され、さらなる保護策の実施も促進できます。
- 優先度の高い脅威の検出、対応および防御を 1 つのコンソールから自動化して予防的に対応できるので、アナリストはタスクを切り替えて作業する必要が減ります。MVISION Insights は、実践的なガイダンスとともに、関連するデータ要素を 1 か所に集めて分析するため、こうした情報を必要な時にいつでも使うことができます。

詳細な知見

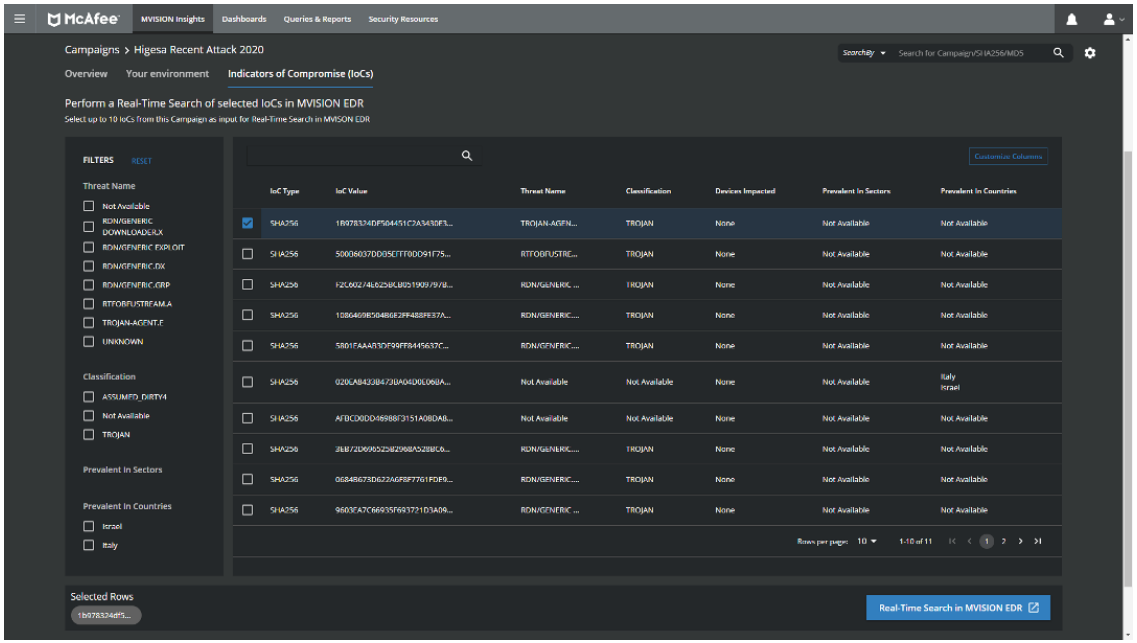

図5. 脅威イベントを深堀りして理解し、組織の防御力を測ります。EDR 機能も利用できます。

MVISION Insights 要件

MVISION Insights は、McAfee® ePolicy Orchestrator® (McAfee® ePO™) ソフトウェア 5.10 (オンプレミスおよび IaaS) および McAfee® MVISION ePO™ (SaaS) によって管理されます。これは McAfee の最新のエンドポイント保護テクノロジである McAfee® Endpoint Security および McAfee® Agent 向けに最適化されています。MVISION Insights が効果的に機能するためには、McAfee Endpoint Security の利用統計情報への同意 (オプトイン) が必要です。

サンプル ユースケース

問題	解決策	結果
自分は標的にされているか？ **これは新しいキャンペーンの亜種か？**	▪ 既知のキャンペーンの脅威アセスメント ▪ 重大な脅威グループや犯罪者の評価 ▪ 厳選された遡及的攻撃分析 ▪ 相対的な保護有効性レポート ▪ ユーザー IoC 遡及的攻撃分析	次の疑問に回答する：脅威にさらされているか？自分を狙う特定の攻撃者がいるか？ 自分を攻撃しそうなキャンペーンがあるか？
全体的なセキュリティ ポスチャは？	▪ エンドポイントからクラウドまでカバーする統合セキュリティ ポスチャ	包括的なセキュリティ対策を評価し、それに基づいて行動
現在の保護対策は十分か？	▪ ローカル保護ポスチャのチェック	現行のセキュリティ ポスチャの評価
保護するためには具体的に何を変えるべきか？	▪ ローカル保護ポスチャのチェック	何をすべきかの規範的ガイダンス
他のセキュリティ機能で分離可能か？	▪ 他のセキュリティ機能で分離または封じ込めるためにパブリッシュ	さらにリスクを低減するため (Data Exchange Layer [DXL] 経由で) 他のセキュリティ機能にアクションを送る

詳細を見る

詳細については、www.mcafee.com/jp をご覧ください。

〒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

McAfee、McAfee のロゴ、MVISION、ePolicy Orchestrator、McAfee ePO は、米国法人 McAfee, LLC または米国またはその他の国の関係会社における登録商標または商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。
Copyright © 2021 McAfee, LLC. 4750_0521
2021年5月