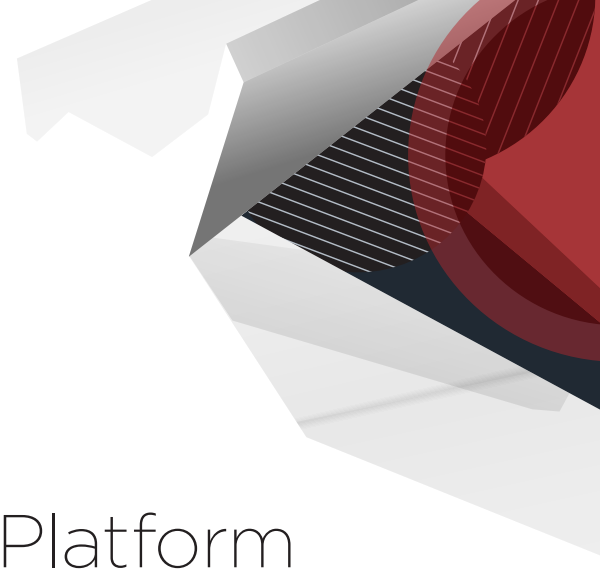
MANDIANT®



データシート

Security Instrumentation Platform

セキュリティ対策の真の効果を測定

ハイライト

- 関連性が高くタイムリーなサイバー脅威インテリジェンスに基づいて、**重要な脅威に優先順位を付ける**
- 現実の攻撃者からの攻撃に対する**現在のセキュリティ・ツールの有効性を診断する**
- 組織のセキュリティ・インフラで**見過ごされているギャップや重複を発見する**
- チームが検知と対応に要する**時間を測定する**
- 最適化できる**可能性の高い部分を特定する**
- 長期間にわたる防御体制の**改善を定量化する**
- 証拠により、投資の**価値を合理的に**役員に示す
- ビジネス全体にわたるセキュリティ体制の状態についての**コミュニケーションを簡略化する**

動的に変化を遂げる今日の脅威環境において、CISOやセキュリティ・チームは企業の資産を保護するために日々課題に直面しています。また、サイバー・セキュリティへの投資の価値と、現在および新規の攻撃者に対するセキュリティ対策の有効性を把握し、その証拠を提示することを求められています。

ペネトレーション・テスト、レッドチーム演習、侵害および攻撃シミュレーションでは不十分です。というのも、CISOや経営陣がリスクやサイバー攻撃への対応プロセスを理解するために必要となる定量可能な証拠をもたらすことができないからです。パフォーマンス・データに基づく証拠なしには、セキュリティ・チームが防御を最適化したり、確信を持ってセキュリティ体制に関する報告をしたりすることはできません。

Mandiant Security Instrumentation Platformは、Mandiantのインテリジェンス主導型セキュリティ対策検証テクノロジーの重要な要素であり、組織が必要とする証拠を提供します。Security Instrumentation Platformは、サイバー・セキュリティ・リスクの診断と管理を行うプラットフォームであり、セキュリティ・チームは重要な資産が常に保護されていることを確認できます。

セキュリティ対策機能の有効性が向上

Mandiant Security Instrumentation Platformは、Mandiantのグローバル脅威インテリジェンスとインシデント対応のデータを活用します。これは、攻撃者の今現在の活動に関する比類のない独自の脅威データと攻撃者の可視性を提供するものです。Mandiantの脅威インテリジェンスとセキュリティ検証テクノロジーを組み合わせることにより、セキュリティ・チームは、組織を標的とする可能性の高い攻撃者や手法を把握し、それに基づいて検証戦略を備えることができます。

Mandiantのインテリジェンス主導型セキュリティ検証テクノロジーは、まず、関連性の高い重要な脅威の優先順位付けを行います。その後、現実の攻撃に対する全体的なセキュリティ・アーキテクチャの有効性を安全に診断し、定量化された個々の証拠を取得します。その結果、現在のセキュリティ・テクノロジーを突破したりすり抜けたりする個別の具体的な攻撃、時には拡張されたキル・チェーン全体が明らかになります。これらの知見を使用して、必要に応じて特定のパフォーマンス・データやベンダーを取り入れながら、最適化すべき対策機能とその方法を判断し、最終的にプログラム全体の改革を実現できます。

Mandiant Security Instrumentation Platformを備えることで、世界中の高度で最新の攻撃者に対する組織のセキュリティ・プログラムの有効性を速やかに定量し、証明することができます。このテクノロジーは、オンプレミス、クラウド、ハイブリッド・アーキテクチャのいずれでも使用できます。

有効性の向上を定量化することによって、企業のリスク許容度に照らしたセキュリティ投資の価値を、経営陣に証明して見せることができます。

Mandiant Security Instrumentation Platformでは、プロセスが自動的かつ継続的に行われるため、プラットフォームが全体的なセキュリティの有効性を厳重に監視、測定している間、セキュリティ・チームはビジネスの戦略的な防御に集中できます。

セキュリティ体制の信頼性を得る

Mandiant Security Validationの専門家は、組織と協力して迅速にプラットフォームを設定し、攻撃者、アラートのソース、具体的なセキュリティ対策機能を結び付けて、深い知識をもたらします。簡単な統合によって、攻撃の振る舞いを安全に実行し、防御スタックのパフォーマンスを可視化できます。

設定が完了したら、Mandiantの膨大なライブラリから、個別のテスト、あるいは事前設定された一連のテストを選択します。このライブラリには、実際の攻撃、攻撃者のTTP（Tactics、Techniques、Procedures）、さまざまなタイプのマルウェアが含まれています。これらのテストは安全に実行されるため、特定のセキュリティ対策機能が適切に動作しているかを迅速かつ継続的に検証できます。テストの実行中は、検知、アラート、見逃し、防御率がダッシュボードにリアルタイムで表示されます。

このプラットフォームは、そのイベントが適切にタイムスタンプされ、適正に解析されているか、また定義されている相関ルールと脅威モデルが実際にアラートを生成したかどうかを検証します。長期間にわたる全体的なセキュリティの有効性の概要を示すレポートも、表示、あるいはエクスポートできます。継続的な検証が常時行われているため、セキュリティ・チームにとっても、経営陣や役員にとっても、プログラムの信頼性を達成、維持するために必要な証拠が得られます。

プラットフォームの詳細

Mandiantのプラットフォームはオープンで、カスタマイズおよび拡張が可能です。セキュリティ対策機能の自動検知と、実際の攻撃バイナリを用いてセキュリティ対策機能を安全にテストするアーキテクチャを提供します。プラットフォームには6つの主要コンポーネントが含まれます。

Director

ダイナミックな本番環境全体にわたる継続的な検証の中央コントローラおよびマネージャーであり、クラウドベース（セキュリティ・アズ・ア・サービス（SaaS））のプラットフォームまたはオンプレミスで、仮想アプライアンスまたはインストール可能なソフトウェアとして使用できます。

アクター

本番環境でテストを安全に実行し、ネットワーク、Windows、MacOS、Linuxのエンドポイント、Eメール、クラウドのセキュリティ対策機能の有効性を検証し、現在のインフラが適正に設定されていることを確認します。

統合

防御テクノロジーとセキュリティ・インフラが統合されており、セキュリティ対策機能の詳細な検証を実行できます。

攻撃ライブラリ

このコンテンツ・ライブラリには、拡張されたキル・チェーンを含む、アタック・ライフサイクルのあらゆる段階の数千もの攻撃が用意されています。これは、Mandiantのグローバルな脅威、攻撃者、侵害に関するインテリジェンスによって裏付けられた、現在および新規の攻撃者の振る舞いやTTPに基づくものです。

フレームワーク

MITRE™ ATT&CKおよびNISTフレームワークに攻撃をマッピングし、有効性とセキュリティ診断プログラムとを簡単に結び付けることができます。Mandiant Security Validationの強みは、そのコンテンツによって組織に関連性の高い攻撃フレームワーク戦術に関する知見が得られるうえ、総合的で関連性の高いテストを行い、正確な結果を得るために、MITRE ATT&CK戦術に対する検証にもそのコンテンツを使用できることです。

ダッシュボードとレポート

ライブのグラフィック・ディスプレイには、組織の環境内で実行されたテストの結果と、経時的な有効性の向上に関するレポートが表示されます。レポートには、実際の定量的データが含まれており、役員への報告にも利用できます（図1）。

図1:ダッシュボードは、アタック・ライフサイクル全体にわたってセキュリティ対策機能を検証し、リスク領域を特定する

インテリジェンス主導型の検証方法

Mandiant Security Instrumentation Platformは、環境ドリフトの自動検知を用いて、セキュリティ対策機能の完全かつ継続的な監視、検証、最適化を行います。この継続的な検証プロセスは、インテリジェンス主導型の5段階の手法によって実行されます(図2)。

図2: Mandiantのインテリジェンス主導型の5段階検証手法

高度な機能

- **Threat Actor Assurance Module(TAAM):**脅威インテリジェンスが実践的なものとなるため、現実の攻撃者、特に組織を標的とする可能性が高い攻撃者に対するセキュリティ対策のパフォーマンスをテストできます。TAAMは、業界大手のサードパーティのインテリジェンス・フィードと統合できます(図3)。
- **Advanced Environmental Change/Drift Analysis:**ITインフラの継続的なモニタリングを実現することで、環境ドリフトをなくし、防御力の低下を防ぐために継続的に検証を行って、組織のセキュリティ・インフラの健全性を確保します。
- **Protected Theater:**マルウェア、ランサムウェア、その他の破壊的な攻撃を安全に実行し、エンドポイントの対策の有効性を検証することで、最新の脅威に対して予防的な保護が可能になります。
- **Email Theater:**Eメール・セキュリティ・プラットフォームで提供されている対策機能をテストします。

図3: Threat Actor Assurance Module（TAAM）

Mandiant Security Validationポートフォリオには複数の導入オプションが用意されています。

- **顧客所有管理モデル:** クラウドベース（SaaS）、またはオンプレミスの仮想アプライアンスとして導入します。
- **完全マネージド型モデルと共同マネージド型モデル:** ビジネス成果に対する顧客の希望に基づいて、Mandiantチームが具体的なユースケースに適合する検証プログラムを構築し、顧客の関係者に詳細なレポートを継続的に提供します。
- **オンデマンド検証:** ユースケース単位で1回限りの検証を購入できます。事前に定義済みの攻撃や攻撃者をブロック、防御する能力を診断し、防御を改善してリスクを低減するために必要となる追加的な調査についての推奨事項が得られます。

Mandiantの脅威インテリジェンスを踏まえたセキュリティ検証

過去15年以上にわたる世界各地での調査、インシデント対応、レッドチーム演習を通じて、Mandiantは脅威インテリジェンスの独自のポートフォリオを構築しました。このポートフォリオは、新たな証拠データ、人間が持つ専門知識、独自の解析ノウハウにより、常時アップデートされています。Mandiantは現在、バランスのとれた以下のソースにより、サイバー脅威インテリジェンスの分野における第一人者となっています。

- Mandiantコンサルティングのインシデント対応を通して収集された**侵害インテリジェンス**
- Mandiantの研究者によって得られた**攻撃者インテリジェンス**
- FireEyeセキュリティ製品による**マシン・インテリジェンス**
- Mandiant Managed Defenseサービスによって得られた**オペレーション・インテリジェンス**

Mandiant Solutionsの詳細については、**www.fireeye.jp/mandiant/security-validation**をご覧ください。

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03-4577-4401 |
Japan@fireeye.com

Mandiant Solutionsについて
Mandiant Solutionsは、世界トップレベルの脅威インテリジェンスと最前線で得られた専門知識を継続的なセキュリティ検証と組み合わせ、セキュリティの有効性を高め、ビジネス・リスクを低減するために必要なツールをお届けします。