MANDIANT®

Security Validation

サイバー・セキュリティの価値を実証

CISOはセキュリティの有効性を証明しなければならない

今日、ビジネス環境のリスクは広く認識されています。CISOとセキュリティ・チームは、企業資産を守り、財務体制やブランドの価値を保護するために、これまでにないプレッシャーにさらされています。攻撃者による重要なシステムへの侵害を防ぐためのサイバー・セキュリティへの投資の価値と効果を、経営陣に対して証明して見せなければなりません。

しかし、セキュリティの有効性を検証し、リスクを定量化し、運用能力を示すために必要なツールがないため、脆弱性スキャナー、侵入テスト、レッドチーム、侵害と攻撃シミュレーションといったものに頼らなければなりません。これらのアプローチは本質的に制限があるため、有効性を十分に評価することができず、組織にとって優先度の高い特定の脅威に関連する知見をタイムリーに得ることもできません。

Mandiant Security Validationはその解決策となります。これは、独自のパフォーマンス・モジュールとMandiant Security Instrumentation Platformで構成された、継続的で自動化されたインテリジェンス主導型のポートフォリオです。[1]

有効性を実証し、サイバー・セキュリティ・プログラムを定量化

適切なセキュリティ検証は5段階で実施されます。これによって、組織や業界を標的にしている攻撃者に関する知識に基づいて、検証すべき重要なポイントと、防御を最適化する方法について知見を得ることができます。

図1: Mandiantのインテリジェンス主導型の5段階検証手法

1 旧称：Verodin Security Instrumentation Platform

この手法では、脅威データをリアルタイムで活用する必要があります。Mandiant Security Validationは、Mandiantの脅威インテリジェンスとインシデント対応データを活用して、攻撃者に対する比類のない可視性を実現し、攻撃者の現時点での行動を明らかにします。インテリジェンス主導型のSecurity Validationによって、セキュリティ・チームは組織にとって優先度の高い脅威を特定し、組織に脅威をもたらし得る攻撃者に関する知識に基づいて検証戦略を作成できます。Mandiantの支援により、セキュリティ・リーダーとそのチームは、テクノロジー、プロセス、人材のすべてにわたって、セキュリティ対策機能の完全かつ継続的な検証を実施できるようになります。

Mandiant Security Validationは、セキュリティ対策機能の検証テクノロジーであるSecurity Instrumentation Platformを使用します。これにより、セキュリティ・チームはセキュリティ対策機能に対して実際の攻撃行動を実行し、高度な攻撃に対する組織のセキュリティ・プログラムの有効性と防御能力を迅速に定量化し、証明できます。

Mandiant Security Instrumentation Platformの基本的機能は次のとおりです。

- 最も重大な脅威や攻撃者へのセキュリティ対策を優先する
- 現実の攻撃者からの攻撃に対するセキュリティ対策機能の有効性を測定する
- Mandiantの比類のない脅威インテリジェンスとインシデント対応データを踏まえた、関連性の高い攻撃を安全に実行する
- 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を発見する
- 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
- 定量可能な証拠により、投資の価値を合理的に役員に示す

Mandiant Security Implementation Platformの高度な機能は次のとおりです。

- **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。
- **Advanced Environmental 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。

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：**クラウドベース（セキュリティ・アズ・ア・サービス（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。

図2：

プラットフォームは、セキュリティ対策機能によって重要なアセットが保護されていることを可視化し、その証拠を生成する

Security Validationのビジネス上のメリット

有効性と投資対効果（ROI）を測定

定量可能なデータを取得することにより、優先される攻撃タイプに対するセキュリティの有効性を高め、全体的なリスク・プロファイルを定量化するために必要な投資について判断できます。また、セキュリティ・チームはこの証拠を用いて、セキュリティへの投資の価値を経営幹部や役員に合理的に説明できます。

合併と買収

合併や買収を進めている企業のセキュリティ対策における重複やギャップを明確に把握できます。支出を合理化することで、整理可能な金額や、合併の結果生じ得るリスクのレベルを計算できます。

セキュリティ人材の雇用とトレーニング

セキュリティ担当者の過去の経験を確認して、学習能力の高さや経験の種類、現実のシナリオの中でそのスキルセットが組織の環境に適するかを診断します。本番環境で実際の攻撃を安全に実行することにより、ITリーダーは、応募者の対応や反応をモニターできます。また、トレーニング演習として定期診断を実行して、セキュリティ・チームの対応が実際の攻撃シナリオに対して十分に迅速か、必要なスキルを備えているかを見ることができます。

ブランドの保護

セキュリティの有効性を予防的かつ継続的に測定することで、侵害や攻撃を受けるリスクを低減し、社会的な信用や顧客のロイヤルティを守ります。

データのプライバシーと保護

顧客データを保護し、規制、社内規定、サードパーティの規定に対するコンプライアンスを確保します。

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。

MANDIANT®