

データシート

Microsoft 365の セキュリティ診断



ハイライト

- 一般的に悪用される設定ミスを**軽減**する
- Microsoft 365への攻撃経路を**減らす**
- 既存の設定に伴う喫緊のセキュリティ・リスクについての知見を**得る**
- 監視、可視性、検知機能を**強化**する
- セキュリティ強化の**優先順位付け**を行う

Mandiant Solutionsが選ばれる理由

Mandiant Solutionsは、2004年以来、サイバー・セキュリティとサイバー脅威インテリジェンスの最前線で活動を続けてきました。FireEye Mandiantのインシデント対応担当者は、世界各地で発生する数々の複雑なセキュリティ侵害事件を現場で経験しています。攻撃者に関するインテリジェンスのソース、マシンで収集されたインテリジェンスのソース、被害者に関するインテリジェンスのソースを組み合わせて活用することにより、攻撃者とそのTTP (Tactics, Techniques, Procedures) を深く理解しています。

概要

クラウドへの移行が進む中、クラウド・プラットフォームやクラウド・サービスに関与するセキュリティ・インシデントは著しく増加しています。中でも、Microsoft 365は利用者数が多く、格納されるデータの価値も高いことから、頻繁に標的にされます。攻撃者はMicrosoft 365テナントを侵害することによって、企業のネットワーク境界を突破する必要なしに、クラウド上の機密データにリモートでアクセスできるようになります。Microsoft 365テナントにアクセスする際に攻撃者が悪用、または侵害するポイントは以下のとおりです。

- 脆弱な認証メカニズムや従来の認証メカニズム
- 適切に設定されていないセキュリティ管理
- 特権アクセス・レベルのアカウント
- パスワードが弱いアカウントや多要素認証を必要としないアカウント

Microsoft 365のリスクを認識し、リスクの低減を図る

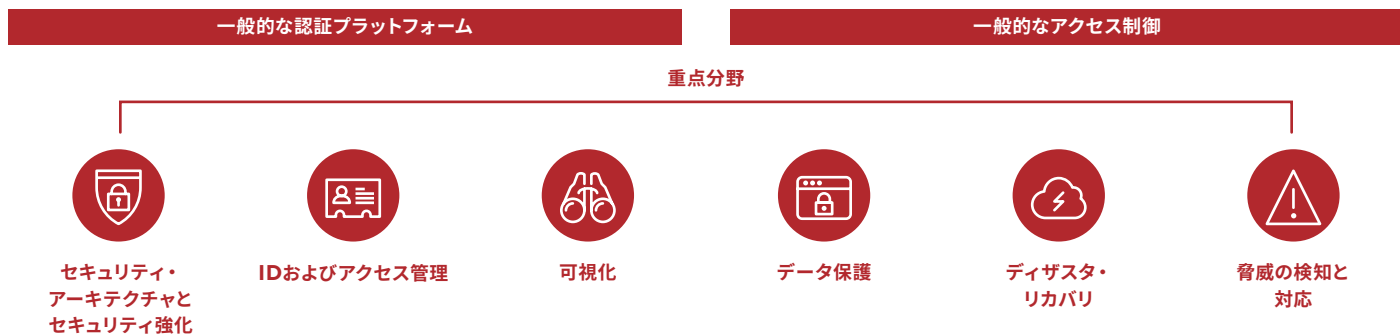
MandiantによるMicrosoft 365向けセキュリティ診断は、組織のMicrosoft 365テナントを攻撃してアクセスを獲得しようと試みる攻撃者に対応してきた、広範な経験に基づいて開発されました。一般的な設定ミス、プロセスの弱点、攻撃手法を予防的に見直して対処することにより、組織は全体的なリスクを低減し、保護の最適化とMicrosoft 365テナント内で生じるイベントの可視性を確保することができます。

この診断は、テナントから攻撃を排除するために必要となる、短期的な封じ込めおよび長期的な復旧セキュリティの管理と設定の両方が基盤になっています。

Mandiantのアプローチ

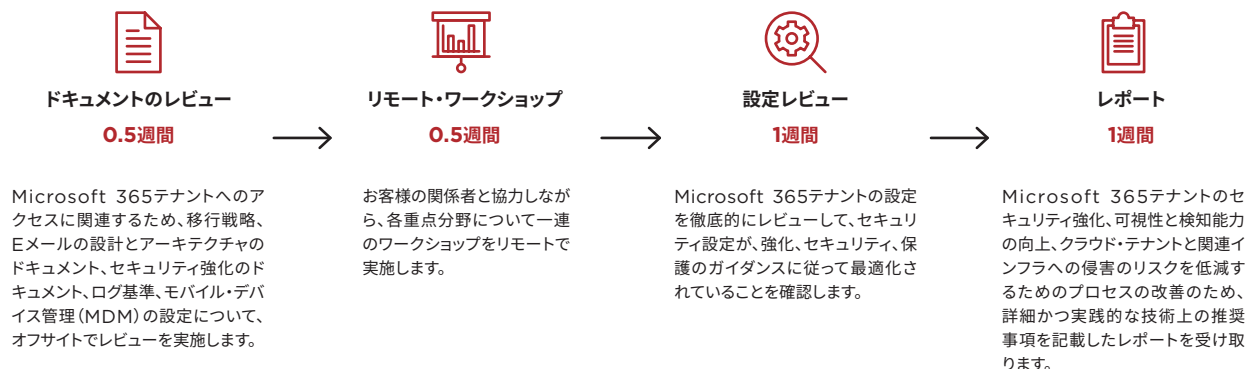
Mandiantセキュリティ診断では、6つの重点分野にわたって、一般的なMicrosoft 365認証プラットフォームとアクセス制御の評価を行います。

- セキュリティ・アーキテクチャとセキュリティ強化
- IDおよびアクセス管理
- 可視化
- データ保護
- ディザスタ・リカバリ
- 脅威の検知と対応



診断期間

Microsoft 365セキュリティ診断は通常3週間で実施され、4つの段階で構成されます。Mandiantのコンサルタントは以下の作業を行います。



成果物

最終的にMandiantの専門家から提供される詳細レポートには、以下が含まれます。

- 既存のMicrosoft 365テナントのセキュリティ設定のスナップショット
- 現在の設定と運用プロセスに沿った、Microsoft 365のセキュリティの具体的なベスト・プラクティス
- 可視性と検知能力を強化するための実践的な推奨事項
- Microsoft 365テナントのセキュリティ体制をさらに強化するための、優先順位を付けた詳細な推奨事項

Mandiant Solutionsの詳細については、www.fireeye.jp/mandiant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

©2020 FireEye, Inc. All rights reserved.
 FireEyeおよびMandiantはFireEye, Inc.の登録商標です。その他のブランド名、製品またはサービス名はそれぞれその所有者の商標またはサービスマークとして登録されている場合があります。M-EXT-DS-JA-JP-000208-02

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。

