データシート

ランサムウェア防御診断

メリット

- ランサムウェアに攻撃を受けるリスクが高いアセットを特定する
- ランサムウェアの標的となるセキュリティの弱点を特定する
- ファイル共有での緩いアクセス・コントロールを特定する
- ランサムウェア関連のタスク管理において、オペレーションの欠陥を認識する
- ランサムウェア攻撃を回避するための実行可能な推奨事項とガイダンスの入手

FireEye Mandiantが選ばれる理由

FireEye Mandiant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。

ランサムウェア防御診断は、ランサムウェア・インシデントへの対応とインシデントからの復旧、および新たなランサムウェアや進化を遂げるランサムウェアに関する脅威インテリジェンスの収集という豊富な経験に基づいて開発されました。

概要

FireEye Mandiantのランサムウェア防御診断では、ランサムウェア攻撃を組織が防御、検知、封じ込め、復旧する能力の有効性を評価します。Mandiantの専門家が、組織のセキュリティ・プログラムの技術的および技術以外の要素を診断し、ランサムウェア攻撃に対するセキュリティ・チームの対応を判定します。

ランサムウェア防御診断では、Mandiantの専門家が、ランサムウェア攻撃が組織内部のネットワークにもたらし得る影響を診断し、流出または損失する可能性のあるデータを見つけ出し、ランサムウェア攻撃を検知、対応するためのセキュリティ・コントロールの能力の長所と弱点をテストします。

方法

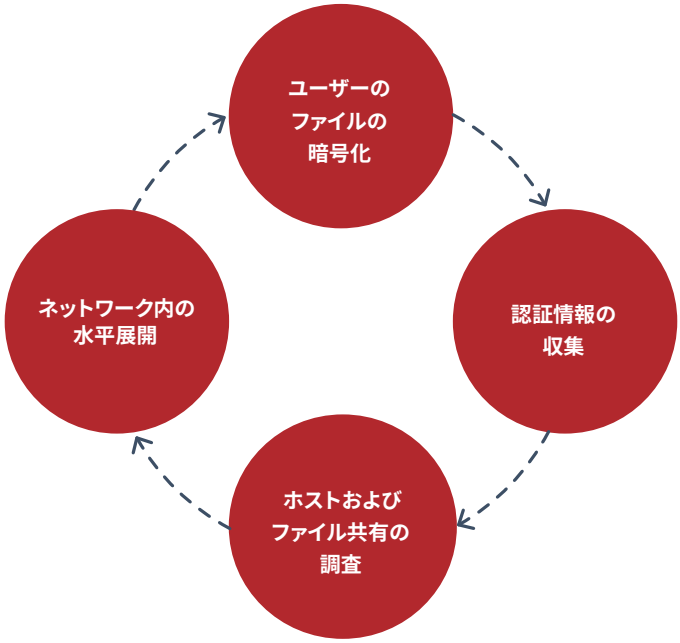
ランサムウェア防御診断には、ドキュメントのレビュー、ログ設定の解析、詳細なワークショップ、実際のランサムウェアの攻撃行動のシミュレーションが含まれます。

ランサムウェア防御診断は、ランサムウェア攻撃に対する4つの主要な能力に重点を置いています。

- **セキュリティ・アーキテクチャ:** ランサムウェア攻撃に対する防御とビジネス業務の継続に必要となる、セキュリティのテクノロジー、管理、ネットワーク
- **対応:** ランサムウェア攻撃に迅速に対応し、封じ込めることができる組織の能力
- **コミュニケーション:** 主要関係者に企業のメッセージを配付するための内部および外部向けコミュニケーション・プロセス。サイバー保険や弁護士との調整も含まれる
- **回復:** ランサムウェア攻撃から復旧または回復するためのプロセスとアプローチ

実際のランサムウェアの攻撃行動のシミュレーションには以下があります。

- ランサムウェアに悪用されるWindowsの脆弱性をスキャン
- ランサムウェアがアクセスする可能性がある、アクセス可能なファイル共有をスキャン
- 発見された脆弱性の悪用や窃取した認証情報の再利用を試みることにより、ランサムウェアの水平展開をシミュレーション
- ネットワーク間のセグメンテーションをテストして、ランサムウェアが以下のような他の環境に広がる可能性を判定
  - 製造工場およびプラントのネットワーク
  - バックアップ・インフラのネットワーク
  - 小売ネットワーク
  - その他のセキュアなネットワーク
- カスタムの非破壊的ランサムウェア・エミュレーション・ツールを使用して大量のファイルの暗号化を模倣することによって、ランサムウェアの暗号化行動をシミュレーション
- 攻撃者がランサムウェア攻撃に使用するテクニックを実行



期間と成果物

通常、ランサムウェア防御診断には1週間かかります。オンプレミスまたはリモートで実行可能です。

診断後、Mandiantからレポートが提供されます。内容は以下のとおりです。

- 長所と改善が必要な点をまとめたエグゼクティブ・サマリー
- テストのプロセスに関する技術的情報
- 深刻度で分類された詳細な調査結果
- 経営幹部向けの状況説明

FireEyeの詳細については、**www.FireEye.jp** 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

©2019 FireEye, Inc. All rights reserved. FireEye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-000285-01

FireEyeについて

FireEyeは、インテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデントレスポンスといった、組織がサイバー攻撃対策をする上での課題となっていた複雑性や負担を解消します。

FIREEYE™