MANDIANT®
ADVANTAGE

THREAT INTELLIGENCE

データシート

MANDIANT ADVANTAGE

Mandiant Advantage Threat Intelligenceは、あらゆる規模の組織に関連性の高い最新のサイバー脅威インテリジェンスを提供します。組織のビジネスにとって重要な脅威への対応に集中し、迅速に行動を起こせます。

昨今の攻撃者は豊富なリソースを揃え、執拗に攻撃を仕掛けてくるため、セキュリティ・チーム全員が注意を払い、知識を深めて対応する必要があります。世界23か国にわたって30以上の言語を理解する300人以上の専門家が独自に構築した**侵害インテリジェンス、マシン・インテリジェンス、オペレーション・インテリジェンス、攻撃者インテリジェンス**を組み合わせることにより、Mandiantはユースケース・ベースの5種類のサブスクリプションを提供しています。組織は**随時更新される脅威インテリジェンス**を活用し、セキュリティ・タスクを迅速かつ正確に実行できます。

MANDIANT ADVANTAGE

Mandiant Advantage Free

一般に知られている脅威と脆弱性を一元管理

脅威インテリジェンスの管理に悩まされているセキュリティ担当者にとってのメリット

- **活発化している攻撃者やマルウェアについての状況認識**
- **CVSSの深刻度スコアを含めた一般に知られた脆弱性についての説明を、リポジトリで一元管理**
- **一般に知られた脅威インジケーターを検索し、Mandiant独自の脅威スコアをブラウザ・プラグインでWebページに直接埋め込み**

脅威インテリジェンスの一元管理は、セキュリティ・アナリストにとって最も時間を取られる作業のひとつと言えます。Mandiant Advantage Freeは、あらゆる規模の組織に対し、一般に知られている攻撃者、マルウェア、脆弱性に関する情報への無料アクセスを提供します。また、悪意のレベルを示すMandiant独自の脅威スコアで補完した脅威インジケーターの可視性に加え、共通脆弱性評価システム（CVSS：Common Vulnerability Scoring System）の深刻度の基準を含めた一般に知られた脆弱性の説明も提供しています。これらを活用することで、セキュリティ担当者は、投資や運用コストなしに、情報に基づいた判断が下せるようになります。

内容

- 攻撃者、マルウェア、脆弱性、活動の動向に関する情報を提供するグローバル・ダッシュボード
- 悪意レベルを示すMandiantによる脅威スコアを付けたオープン・ソースのインジケーターへのアクセス
- オープンソース・インテリジェンス（OSINT）ベースの脆弱性の表示とスコアリング
- Mandiantの専門家の判定とコメント付きのニュース解析
- ポータルおよびブラウザ・プラグイン経由で脅威インテリジェンスにアクセス可能

MANDIANT ADVANTAGE

Mandiant Advantage Security Operations

SOCの効率と効果を高める

セキュリティ・アナリスト、インシデント対応担当者、セキュリティ運用マネージャー、インテリジェンス・アナリストにとってのメリット

- **アラートの優先順位付けとトリアージ:** 随時更新される脅威インテリジェンスを活用して、セキュリティ・イベント情報に優先順位を付け、コンテキストを把握できます。それによって、アラート疲れが軽減され、SOCの全体的な効率が向上します。
- **隠れた脅威を検知:** インジケーターをダウンロードして検知ツールを拡張することにより、環境内に潜む攻撃者やマルウェアの活動を発見します。
- **迅速な対応:** MITRE ATT&CKに基づく攻撃者の振る舞いに関する知見によって、セキュリティ・アナリスト・チームは潜在的な攻撃活動の進行を把握し、適切な対応体制を構築できます。

セキュリティ・オペレーション・センター（SOC）の担当者は、次々と生じるセキュリティ・イベントに追われ、常に注意を払い、手間のかかる調査を手作業で行う必要に迫られています。Mandiant Advantage Threat Intelligence Security Operationsのサブスクリプションは、セキュリティ・アナリストとインシデント対応担当者に対し、攻撃者、マルウェア、脆弱性トラッキングに関する最新情報を提供します。アラートの優先順位付けや、脅威イベントの裏に隠された攻撃者とその能力、攻撃の動機の理解に役立ちます。SOCが生成したアラートをMandiantのリソースおよびオープンソース・インテリジェンス（OSINT）のインジケーターと相関分析することによって、トリアージ、調査、対応に当たる間、セキュリティ・チームは直接的なガイダンスを得ることができます。これによって、セキュリティのスピードと有効性が向上し、全体のアラート疲れが軽減されます。さらに、Security Operationsのサブスクリプションでは、攻撃者やマルウェアに関する詳細なインジケーター・データが提供されるので、セキュリティ・チームは新たなサイバー脅威の検知履歴を把握できます。こうした情報は、Mandiant AdvantageやAPIを通じて利用可能です。

内容

- Mandiant Advantage Freeの機能
- MITRE ATT&CKマップ、オブジェクト・エクスプローラーおよびインジケーターのダウンロードによる、攻撃者とマルウェアのダイナミックなピボット表示
- 悪意レベルのスコア指標を含む、Mandiantが把握しているインジケーター（IP、ドメイン、ファイル・ハッシュ、URL）へのアクセス
- Mandiantの専門家の判定とコメント付きのニュース解析
- 四半期ごとに開催される説明会と基本サポート（プロビジョニングとサービス導入）
- ポータル、ブラウザ・プラグイン、API経由で脅威インテリジェンスにアクセス

MANDIANT ADVANTAGE

Mandiant Advantage Fusion

セキュリティ組織全体をサポートする総合的な脅威インテリジェンス

メリット

- **未知のリスクを発見する：**最前線で得られた最終的なインテリジェンスへの、スケーラブルでカスタマイズ可能なアクセスが得られます。Mandiantの侵害インテリジェンスを活用し、組織の境界の外側にあるグローバルな脅威を特定できます。
- **情報に基づいたサイバー・セキュリティ体制：**脆弱性、攻撃者とその活動、組織のビジネスへの潜在的な影響についての包括的な状況認識によって、セキュリティ戦略を改善します。
- **優先順位を理解する：**攻撃が起こった際に組織にとって重要度の高い脅威を特定して瞬時にアクセスし、セキュリティ対応に優先順位を付けて攻撃を効果的に防御できるので、アラート疲れが軽減されます。
- **脅威のリスクを低減：**セキュリティ対策機能を強化し、Red Team演習で攻撃者の具体的な戦術をエミュレートします。

セキュリティ・チームが攻撃者についての知識を増やそうとするときに起こりがちなのは、ベンダーの影響を受けているものも含めた大量の公開情報を調べてデータ過剰になり、信頼できる未知のデータを組織内で発見した脅威プロファイルに照らし合わせようとするといった状況です。Mandiant AdvantageのFusion Subscriptionは、セキュリティ・チームに必要となる脅威インテリジェンスの唯一のソースとなります。このサブスクリプションでは、現在、過去、未来の脅威活動を含む、Mandiant Threat Intelligenceへの完全な無制限アクセスが得られます。Fusionは、サイバー犯罪、サイバーエスピオナージ、戦略的インテリジェンス、サイバー・フィジカル・インテリジェンス、および攻撃者のオペレーションに関するインテリジェンスといった脅威の複数の側面を組み合わせた、脅威状況に関する比類のない戦略的視点をセキュリティ・チームに提供します。Mandiantの専門家による戦略解析、FireEyeのグローバル・テレメトリー、Mandiantのインシデント対応、テクニカル・リサーチ調査結果に基づいた何千件ものFINISHED INTELLIGENCE（FINTEL）レポートに、1つの検索画面からアクセスできます。

内容

- Mandiant Advantage Free、Security Operations、Vulnerability、Digital Threat Monitoring機能
- レポートのタイプ、リージョン、業種、攻撃者、マルウェア名によるフィルター機能
- 戦略的なものから戦術的なものまで、解析結果とコンテキスト情報を網羅した最終的なインテリジェンスのレポート

MANDIANT ADVANTAGE

Mandiant Advantage Vulnerability（追加モジュール）

最大限まで攻撃経路を減らす

脆弱性アナリスト、IT/システムやデータの所有者、リスク・マネージャー、インテリジェンス・アナリストにとってのメリット

- **可視性：**テクノロジー、攻撃者、エクスプロイト・ソース別に脆弱性データを見ることができます。
- **優先順位付け：**リスクとエクスプロイトの格付けによってデータを解析することで、その時点で最も重要な脆弱性に集中できます。
- **通知：**ゼロデイ脆弱性の通知を受け取ります。
- **インストールが簡単：**ブラウザ・プラグインまたはAPI経由で、組織の脆弱性スキャナーに統合できます。

ITインフラが拡大し、新たなアプリが登場し、物理的ロケーションが多様化する中、組織の環境内に存在する対処すべき脆弱性は膨大な数に上り、脆弱性リスク・アナリストは疲弊してしまいます。脆弱性の情報を解析するのは手間のかかるプロセスであり、簡略的な脆弱性評価システムを備えている場合でも、どこから手を付けるべきか判断するのが難しいことがあります。Mandiant AdvantageのThreat Intelligence Vulnerabilityサブスクリプションには、悪用されやすいか、悪用される可能性が高いか、脅威や被害はどの程度かといった基準に基づく独自のスコアリング・システムが含まれています。これによって、セキュリティ・チームは、発見された脆弱性に対してエンタープライズ規模で評価、優先順位付け、修正を行うことができます。

内容

- Mandiant Advantage Freeの機能
- Mandiantの脆弱性表示とスコアリング：エクスプロイトの格付け、リスク評価、ゼロデイ診断、最前線の専門家が観察した攻撃活動など
- 包括的な脆弱性レポート：CVE ID、脆弱性テクノロジー、エクスプロイトの経路、関連レポートなど
- 四半期ごとに開催される説明会と基本サポート（プロビジョニングとサービス導入）

MANDIANT ADVANTAGE

Mandiant Advantage Digital Threat Monitoring（追加モジュール）

外部からの脅威に対して早期に警告

インテリジェンス・アナリスト、顧問弁護士、広報/コミュニケーション担当者、役員および経営陣にとってのメリット

- **外部の脅威を可視化：**ダークWebを含め、組織の境界の外側にあるアセットに対する脅威を特定します。
- **セットアップが簡単：**組織が定義した検索のパラメーターを用いて、複数のフォーラム、ソーシャル・メディア、ペースト・サイト、攻撃者関連の投稿を、Advantageが継続的に監視します。
- **高い信頼性：**業界で信頼の高い保護されたポータルにより、過検知や検知漏れを低減します。
- **迅速な対応：**インシデント対応体制を整えておくことで、被害の拡大を防ぎ、組織のアセットや情報を守ります。

従来のセキュリティ対策は、ネットワーク内に存在するアセットやイベントに焦点を合わせたものが一般的でした。しかし、さまざまなものが複雑につながり合う現在では、組織のブランド、個人情報、パートナー・コミュニティなど、組織のネットワーク境界を越えたところにあるアセットを保護する必要もあります。Mandiant Advantage Threat IntelligenceのDigital Threat Monitoringサブスクリプションでは、組織のアセットがさらされる外部の脅威を早期に可視化できるほか、ダークWebモニタリングで安心感が得られ、非現実的な大量の手作業も排除できます。ブランド、インフラ、重要度の高いパートナーシップを脅かすリスクを防御します。カスタマイズされたキーワード検索条件を使用して、オープンWeb、ディープWeb、ダークWebにわたって、侵害や漏洩、デジタル脅威を特定します。潜在的に重大な意味を持つ脅威を自動的に検索、解析し、脅威アラートを生成します。

内容

- Mandiant Advantage Freeの機能
- 組織に合わせたスケーラブルな偵察とダークWebの監視を実現する、カスタマイズされたキーワード検索ツール
- マネージドDTM、オンデマンド・サポート、Expertise On Demandを介した、セットアップ、トリアージ、調査のためのMandiantアナリストへのアクセス（オプション）
- アラート・ダッシュボード経由の脅威アラート：ステータス、ソース、深刻度の属性、監視対象のアセットの管理に役立つ貴重な知見
- 四半期ごとに開催される説明会と基本サポート（プロビジョニングとサービス導入）

MANDIANT ADVANTAGE THREAT INTELLIGENCEのポートフォリオ

アクセス・タイプ	FREE	SECURITY OPERATIONS	FUSION
Mandiant Advantageプラットフォームとブラウザ・プラグイン	●	●	●
API		●	●
インジケーター - オープン・ソース - Mandiantスコアリング付き	●	●	●
攻撃者 - オープン・ソースおよび公開	●	●	●
マルウェアおよびマルウェア・ファミリー - オープン・ソース	●	●	●
リアルタイム・ダッシュボード - 攻撃者、マルウェア、脆弱性	●	●	●
インジケーター - Mandiantの独自データ - スコアリングとコンテキスト付き		●	●
攻撃者 - Mandiantの独自データ - UNC、Temp、APT、FIN		●	●
マルウェアおよびマルウェア・ファミリー - Mandiantの独自データ		●	●
攻撃者とマルウェアのライブ・ピボット表示 - MITRE ATT&CK、グラフ		●	●
公開 / 既知の脆弱性の説明	●	●	●
Mandiantによるリスクとエクスプロイトの格付け	+ VULNERABILITYモジュール		●
Mandiantの脆弱性解析	+ VULNERABILITYモジュール		●
ダークWebモニタリング	+ DIGITAL THREAT MONITORING		●
リサーチ・ツールとアラート	+ DIGITAL THREAT MONITORING		●
ニュース解析	●	●	●
四半期ごとに開催される説明会		●	●
戦略的レポート - リージョン、業種、トレンド			●
攻撃者の動機、手法、ツール、振る舞いに関するレポート			●
脅威活動に関するアラート、新たな脅威、脅威動向レポート			●
Mandiantリサーチ・レポート			●

脆弱性とDigital Threat Monitoringは個別に購入可能です。

業界で最も包括的なサイバー脅威インテリジェンスを提供するMandiant Advantageについての詳細は、**www.fireeye.com/advantage**をご覧ください。

MANDIANT® ADVANTAGE

サイバー攻撃が高度化の一途をたどり、その戦術も急速に変化を遂げる中、サイバー環境はますます複雑さを増していきます。攻撃者によるビジネス・リスクを予防的に低減するためには、タイムリーかつ適切なインテリジェンスを活用した、継続的な検証テクノロジーが必要です。FireEyeの傘下にあるMandiant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インシデント対応データを継続的なセキュリティ検証プラットフォームと組み合わせ、組織が導入しているテクノロジーにかかわらず、セキュリティの有効性を高め、組織のリスクを低減するために必要なツールをお届けします。

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

I-EXT-DS-JA-JP-000350-02