MANDIANT
NOW PART OF Google Cloud

MANDIANT ADVANTAGE
データシート

脅威インテリジェンス

ハイライト

脅威インテリジェンスを管理する必要のあるセキュリティ担当者にとってのメリット

- 増加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公知の脆弱性についての説明を、リポジトリで一元管理
- 公知の脅威インジケーターを検索し、Mandiant独自のインジケーター信頼度スコアをブラウザ・プラグインでWebページに直接埋め込める機能

昨今の攻撃者は執拗に攻撃を仕掛けてくるため、セキュリティ担当者全員が注意を払い、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。組織は分単位で更新される最新の脅威インテリジェンスを活用し、セキュリティ・タスクをより迅速かつ的確に実行できます。

Mandiant Advantageが提供するサブスクリプションでは、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。組織は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。

Mandiant Advantage Threat Intelligence無償版

公知の脅威と脆弱性を一元管理

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1つと言えます。Mandiant Advantage Threat Intelligence無償版は、あらゆる規模の組織に対し、公知の攻撃者、マルウェア、脆弱性に関する情報への無償アクセスを提供します。また、悪意のレベルを示すMandiant独自のインジケーター信頼度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公知の脆弱性についての説明も提供しています。このため、セキュリティ担当者は追加の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
- Mandiant独自のインジケーター信頼度スコアで測定するオープンソース・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

メリット

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：**分単位で更新される最新の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。このため、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検知します。
- **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、適切な対応態勢を構築できます。

Mandiant Advantage Threat Intelligence Security Operations

SOCの効率と効果を高める

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。このため、セキュリティのスピードと有効性が向上し、全体的なアラート疲れが軽減されます。自社の業種や地域、同僚を標的とする最新かつ影響の高い脅威活動を把握することで、自信を持って脅威を予測・特定し、対応できます。また、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ため、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 Threat Intelligence無償版
- 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動的ピボット表示
- 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
- 四半期ごとのブリーフィングと基本サポート（プロビジョニングとサービス導入）
- 最もアクティブで関連性の高い脅威活動に対してリアルタイムの可視性を提供

メリット

- **未知のリスクを検知する：**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防御：**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できます。
- **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ため、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、レッドチーム演習で攻撃者の具体的な戦術をエミュレートします。

Mandiant Advantage Threat Intelligence 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

セキュリティ・チームは、攻撃者についてもっと把握しようとするあまり、ベンダーの影響を受けていることの多い、公開されている大量の脅威情報を調べるという状況に陥りがちです。その結果、データ過剰になり、未知の信頼データを組織内で検知した脅威プロファイルに照らし合わせる必要が出てきます。Mandiant AdvantageのFusionサブスクリプションは、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、サードパーティのグローバル・テレメトリー、Mandiantのインシデントレスポンス、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 Threat Intelligence無償版、Security Operations、Vulnerability、Digital Threat Monitoring機能
- レポートのタイプ、地域、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レポート

メリット

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

- **可視化：**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。

Mandiant Advantage Vulnerability（追加モジュール）

最大限まで攻撃経路を減らす

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、簡単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の判断が難しいことがあります。Mandiant Advantage Threat Intelligence Vulnerabilityの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
- 四半期ごとのブリーフィングと基本サポート（プロビジョニングとサービス導入）

メリット

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資産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：**業界でも信頼性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：**インシデント対応態勢を整えておくことで、被害の拡大を防ぎ、組織の資産や情報を守ります。

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

従来のセキュリティ対策は、ネットワーク内に存在する資産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資産を保護する必要もあります。Mandiant AdvantageのDigital Threat Monitoringサブスクリプションでは、組織の資産がさらされる外部の脅威を早期に可視化できるだけでなく、ダークWebモニタリングにより不安が解消されます。この結果、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できます。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できます。そこから、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できます。

内容

- 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、監視対象の資産の管理に役立つ貴重な知見
- 四半期ごとのブリーフィングと基本サポート（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

	無料版	Security Operations	Fusion
アクセス・タイプ			
Mandiant Advantageプラットフォームとブラウザ・プラグイン	○	○	○
API	○	○	○
データ・アクセス			
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		○	○
攻撃グループ - Mandiantの独自データ - UNC、Temp、APT、FIN		○	○
マルウェア、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		○	○
攻撃グループの活動データとその表示		○	○
脆弱性			
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		○
DIGITAL THREAT MONITORING (DTM)			
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		○
解析および攻撃者インテリジェンス			
ニュース解析	○	○	○
四半期ごとのブリーフィング		○	○
戦略的レポート - 地域、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			○

VulnerabilityとDigital Threat Monitoringは個別に購入可能です。

詳しくはwww.Mandiant.jp/intelligenceをご覧ください。

マンディアント
〒106-0032
東京都港区六本木６丁目１０番1号
六本木ヒルズ森タワー

*Mandiantは現在、Google Cloudの一部です。

Mandiantについて
2004年の設立以来、Mandiantはセキュリティに真摯に取り組む組織にとってのパートナーとして信頼を得ています。現在、業界トップクラスの脅威インテリジェンスと専門の経験、知見をもとに、ダイナミックなソリューションを提供することで、効果的なセキュリティプログラムの構築とサイバー防御態勢の確立においてお客様組織を支援しています。

MANDIANT
NOW PART OF Google Cloud