Cisco AMP Threat Grid - クラウド

Cisco® Advanced Malware Protection（AMP）Threat Grid は、マルウェア分析およびコンテキストリッチ インテリジェンスという 2 つの優れたマルウェア対策ソリューションを組み合わせた製品です。これを活用すると、セキュリティ担当者はサイバー攻撃にプロアクティブに備え、攻撃を受けてもすばやく回復することができます。

製品概要

Cisco AMP Threat Grid は非公開コミュニティからマルウェアをクラウド ソーシングし、静的/動的（サンドボックス）分析を含む独自の高度なセキュリティ手法に従ってあらゆるサンプルを分析します。数億もの他の分析済みマルウェアのアーティファクト、マルウェア攻撃、キャンペーン、およびその配布状況をグローバルで把握できるよう分析結果を関連付けます。セキュリティ チームは、サンプルの動作と特性を、これまでの履歴およびグローバル コンテキストの何百万ものサンプルと関連付け、振る舞いを完全に理解することができます。こうしてアナリストは、高度なマルウェアによる標的型攻撃や、より広範な脅威に対して、効果的に防御できます。AMP 脅威グリッドによる、重要な動作インジケータの特定や脅威スコアの割り当てなどの詳細なレポートを通じて、迅速に優先付けし、高度な攻撃から回復することができます。

機能と利点

AMP Threat Grid の機能と利点を表 1 に示します。

表 1. 機能と利点

機能	利点
高度な分析	• マルウェアの動作に関する包括的なセキュリティの洞察を提供します。 • サンプル ソース、および AMP Threat Grid の包括的データベースに保管された関連性のある動作に直接アクセスするためのリンクが備わっています。 • すべての情報、および詳細な調査のための分析結果に簡単にアクセスできる機能を提供します。
高度な侵入兆候	• 450 を超える、非常に精度が高く、実用的で高度な侵入兆候を低い誤検出率で分析します。 • 高度な静的/動的分析によって、数多くのマルウェア ファミリや悪意ある動作を含む包括的な指標を生成します。 • 脅威に関する最も広範なコンテキストを提供し、信頼性のある判断を迅速に下せるようにサポートします。
Glovebox	• ネットワークが感染するリスクなくマルウェアを分析できる安全な環境を提供します。 • アナリストがアプリケーションを開いたり、ワークフロー プロセスを複製したりすることでマルウェアの動作を把握することができます。仮想マシンを再起動することも可能です。
脅威スコア	• 脅威の優先順位付けが改善されるため、マルウェア アナリスト、インシデント対応担当者、セキュリティ エンジニアリング チームの効率が向上し、AMP Threat Grid フィードを使用する製品の精度が高まります。 • 観察されたアクション、履歴データ、頻度、クラスタリング指標およびサンプルの正確さと重大度を考慮した独自の分析とアルゴリズムにより、脅威スコアを自動的に算出します。 • 信頼性の高い脅威の優先度を定め、各サンプルの悪意ある動作レベルを示します。
統合用 API	• 既存のセキュリティおよびネットワーク インフラストラクチャを利用して、脅威インテリジェンスを素早く簡単に運用可能にできます。 • Cisco AMP Threat Grid の Representational State Transfer（REST）API により、素早く簡単に統合できます。 • ゲートウェイ、プロキシ、セキュリティ情報とイベント管理（SIEM）プラットフォームを含む、多数のサードパーティ製品向けの統合ガイドが用意されています。
標準のフィード形式	• フィードは標準化されているため、規格化された多数の形式（JavaScript Object Notation（JSON）、Cyber Observable Expression（CybOX）、Structured Threat Information Expression（STIX）、カンマ区切り値（CSV）など）に簡単に統合したり、Snort ルールとして統合したりできます。 • 特定のセキュリティ製品向けに、フィード形式をカスタマイズして利用できます。 • 経時的な傾向を容易かつ継続的に追跡して、実用的なレポートを生成できます。

高度なインテリジェンス、分析、レポート

AMP Threat Grid のクラウドベースのサービスは、最も強力でコンテキストリッチな脅威インテリジェンスを提供します。Threat Grid は、数百万ものファイルを安全に分析し、数億もの他の分析済みマルウェア アーティファクトとこれらのファイルとの関連を調べます。マルウェアの履歴またはグローバルな状態を把握できます。データのピボット機能を利用することでアナリストは、害がないように装っている悪意のあるファイルを特定し、詳細に分析することができます。さらに、強力な検索機能、関連性検出機能、レポート機能により、マルウェア アーティファクト、指標、サンプルに関する詳細な情報を入手できます。詳細な分析レポートには、ネットワーク トラフィックとマルウェア アーティファクトを含め、あらゆるマルウェア サンプル アクティビティが示されます。

包括的なプレミアム フィード コンテンツ

Cisco AMP Threat Grid は、閉じたパートナー/カスタマー コミュニティからマルウェアをクラウド ソーシングし、これによってマルウェアの攻撃、動向、流通を大局的に把握できます。毎月、何百万ものサンプルを分析して、テラバイト規模の豊富で実用的なコンテンツを明確にカテゴリ化し、簡単に取り込める脅威インテリジェンス フィードとして抽出します。これにより、広範囲にわたる多種多様な脅威を効果的に防ぎ、攻撃による被害を減らすことができます。AMP Threat Grid には、事前にパッケージ化されたプレミアム フィードが用意されています。これらのフィードは、たとえば次に示すような多様な脅威を扱います。

- 各種のトロイの木馬、リモート アクセス型のトロイの木馬（RAT）、マルウェア ファミリ（他のマルウェアを拡散させ、実行可能ファイルのダウンロードなど特定の動作を示すことが知られている）など。
- アウトバウンド ネットワーク通信の確立を試みて、異常なネットワーク アクティビティを示すマルウェア。例としては、悪意あるネットワーク アクティビティを開始する PDF ファイルや Microsoft Office ドキュメント、さまざまなプロトコルとチャネルで通信するマルウェア、非標準または一致しないネットワーク プロトコルの使用、既知のシンクホールを使った通信が挙げられます。AMP Threat Grid では、特定の侵入兆候を使ってフィードを生成します。これらの指標には、アウトバウンド通信の判別に利用されるネットワーク指標などがあります。
- ホスト上の悪意あるアクティビティ。たとえば、Windows ホスト ファイルやダイナミック リンク ライブラリ（DLL）の改変、悪意あるファイルをインストールして、レジストリを変更することなくホストに存続させるハイジャック手法などです。
- AMP Threat Grid によって高い脅威スコアが算定されたマルウェア。

表 2 に、Cisco AMP Threat Grid でサポートされるプラットフォームおよび Cisco IOS® ソフトウェア リリースをリストします。

表 2. サポートされるプラットフォームおよびオペレーティング システム

製品ファミリ	サポートされるプラットフォーム
AMP Threat Grid ポータル	• Windows XP • Windows 7（32 ビットおよび 64 ビット）
AMP Threat Grid の動的分析	分析でサポートされるファイル タイプ： • Portable Executable 32-bit（PE32）ファイル：実行可能ファイル（exe）、ダイナミック リンク ライブラリ（dll） • Java アーカイブ（jar） • Adobe Portable Document 形式（PDF） • Microsoft Office ドキュメント：rtf、doc(s)、xls(x)、ppt(x) • ZIP（zip）（コンテナとして） • URL：インターネット ショートカット ファイル（url） • HTML ドキュメント

ライセンス

AMP Threat Grid には、詳細な分析を行って結果を示す機能があります。これには、プロセス マッピングとレジストリの変更、ネットワーク接続、環境内でのマルウェア実行のビデオが含まれます（該当する場合）。分析したインテリジェンス データのバッチ フィードにアクセスすることができます。また、さらに広範囲の AMP Threat Grid データからカスタム フィードを作成することも可能です。

さらに、AMP Threat Grid のお客様は、クラウド ポータルからサンプルを直接送信することも、AMP Threat Grid API を使って自動送信することもできます。すべてのクラウド サービスの要素は、1 年または 3 年のコンテンツ サブスクリプションとしてライセンスが許諾されます。サブスクリプション レベルには、レベルごとのユーザ アカウント数と、AMP Threat Grid クラウドに分析対象として送信する 1 日あたりのファイル数が含まれます。

表 3 に、調査/分析用 AMP Threat Grid ポータルへのログイン権限を持つよう作成されたアナリスト アカウントの数と、静的/動的分析の対象として手動または API を介して Threat Grid クラウドに送信できるファイルの数をリストします。

表 3. アナリスト アカウント ライセンス数および分析対象として送信可能なファイル数

ライセンス レベル：アカウント数	1 日に送信できる最大ファイル数
5	500
10	1,500
25	2,500
100	10,000

シスコとパートナーによるサービス

シスコおよびシスコ認定パートナーによるサービスは、AMP Threat Grid のプレミアム脅威フィードおよび Representational State Transfer（REST）API との統合を計画および実装するお客様を支援します。計画/設計サービスは、既存のインフラストラクチャ、AMP Threat Grid プレミアム フィード形式、および運用プロセスに応じて提供されるため、高度な脅威フィードを最大限にご利用いただけます。

Cisco Capital

目標の達成を支援するファイナンス

Cisco Capital は、お客様が目標の達成と競争力の維持に必要なテクノロジーを導入できるよう支援します。お客様の CapEx を削減し、成功を加速させ、投資金額と ROI を最適化します。シスコ キャピタル ファイナンス プログラムにより、ハードウェア、ソフトウェア、サービス、および関連するサードパーティ製機器を柔軟に購入することができます。また、それらの購入を 1 つにまとめた計画的なお支払い方法をご用意しています。Cisco Capital は 100 ヵ国以上でサービスを利用できます。詳細はこちら

関連情報

Cisco AMP Threat Grid 統合マルウェア分析および脅威分析に関する詳細については、http://www.cisco.com/web/JP/solution/security/advanced-malware-protection/index.html を参照してください。

この資料の記載内容は 2017 年 3 月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C78-733495-01JA 17.03