At-A-Glance

Cisco Advanced Malware Protection Threat Grid

利点

- 既存のセキュリティ テクノロジーとリソースを活用して**高度な攻撃を阻止**
- **セキュリティ チームとインシデント対応チームの有効性を向上**
- **セキュリティ侵害をより短時間で発見し、セキュリティ インシデントにより素早く対応**

「AMP Threat Grid は革命的です。全く新しい方法で、正確かつコンテキスト リッチなマルウェア分析と脅威インテリジェンスを活用することで、組織を高度なサイバー攻撃から守れるようになります。」

Jon Olstik
ESG グループ

図 1.　セキュリティ チームで Cisco AMP Threat Grid を利用する方法

近年、ますます多くの企業が、数々の一般的なマルウェア攻撃や高度なマルウェア攻撃にさらされていることを認識するようになりました。多くのセキュリティ担当者や IT 管理者は、このような攻撃を効果的に検知しようと苦労しています。優先度の高い非常に危険な攻撃を見極めるのは至難の業です。

その苦労から解放される時が来ました。Cisco® Advanced Malware Protection (AMP) Threat Grid を使用すると、メール ゲートウェイ、セキュリティ情報とイベント管理 (SIEM)、GRC (Governance, Risk management, and Compliance) プラットフォームをはじめとする既存のネットワークおよびセキュリティ インフラストラクチャに、マルウェア分析と脅威分析の統合機能が組み込まれます。大規模な静的および動的マルウェア分析ソリューションを利用することで、マルウェアを検知して脅威を軽減するためのタイムリーかつコンテキスト リッチで実用的なインテリジェンスが得られます。

Cisco AMP Threat Grid は世界中のさまざまな場所に配備されており、セキュリティ オペレーション センターやインシデント対応チームがより効果的かつ一貫性のある措置を取るのに役立ってきました (図 1)。

マルウェアと戦うために不可欠な 2 つの武器：マルウェア分析と脅威インテリジェンスの統合

Cisco AMP Threat Grid は、コンテキストに基づく分析を駆使し、ほぼリアルタイムで正確に攻撃を検知します。この製品は、何百万ものファイルを分析し、他の何億ものマルウェアの分析済み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。これにより、お客様はマルウェアの攻撃、動向、および流通を大局的に把握できるようになります。

次のステップ

クラウド対応 Cisco AMP Threat Grid について詳しくは、http://www.cisco.com/web/JP/product/hs/security/amp-threat-grid-cloud/index.html にアクセスしてください。

Cisco AMP Threat Grid アプライアンスについて詳しくは、http://www.cisco.com/web/JP/product/hs/security/amp-threat-grid-appliances/index.html にアクセスしてください。

Cisco AMP Threat Grid には次のメリットがあります。

- 主な動作指標を認識して脅威スコアを判定できるため、優先的に対処すべき高度な攻撃を素早く見定めて攻撃から回復することができます。
- チームの防御力が強まり、優先的な問題を迅速、効果的、かつ確実に見定め、対応できるようになります。
- マルウェア対策機能を自動化して、検出/対処するまでの時間を短縮できます。
- 既存のセキュリティ インフラストラクチャ（SIEM、侵入検知システム、ゲートウェイ、プロキシなど）にプレミアム フィードを容易に統合して、マルウェアの検出およびブロックにかかる時間を短縮できます。

Cisco AMP Threat Grid は、高度な攻撃を的確に検出して防御します。さらに、堅牢な検索機能、関連性検出機能、レポート機能により、現在および過去のマルウェア 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。

C45-733452-00-J 12/14