プライバシーとサンプルの可視性

この章では、Threat Grid へのサンプル送信に関するプライバシーとサンプルの可視性モデルについて説明します。説明する項目は次のとおりです。

プライバシーとサンプルの可視性の概要

分析のため Threat Grid アプライアンスにサンプルを送信する際、コンテンツのプライバシーが重要な考慮事項となります。機密文書やアーカイブタイプの資料が分析用に送信される場合、プライバシーは特に重要な考慮事項になります。機密情報を見つけることは、特に検索 API を使用して Threat Grid アプライアンスにアクセスできるユーザにとって、比較的簡単である可能性があるためです。

Threat Grid へのサンプル送信に関するプライバシーとサンプルの可視性モデルは次のとおりです。

- サンプルは、プライベートに指定されていない限り、送信者の組織外のユーザに表示されます。
- プライベートサンプルは、サンプルを送信したユーザと同じ組織内の Threat Grid ユーザのみが閲覧できます。

統合のプライバシーと可視性

プライバシーとサンプルの可視性モデルは、統合によって送信されるサンプルに関連した Threat Grid アプライアンスで変更されます。統合とは、E メール セキュリティ アプライアンス（ESA）、Web セキュリティアプライアンス（WSA）および他のデバイスなどのシスコ製品や、サードパーティのサービスのことです（CSA 統合という用語は、Cisco Sandbox API 経由で Threat Grid アプライアンスに統合（または登録）されている、ESA/WSA その他のシスコ製アプライアンス、デバイス、サービスを意味します）。

Threat Grid アプライアンスでのすべてのサンプル送信は、デフォルトでパブリックに設定されるため、所属する組織にかかわりなく、統合を含む他のすべてのアプライアンスユーザが表示できます。アプライアンスのすべてのユーザが、他のすべてのユーザが送信したサンプルのあらゆる詳細を確認できるということです。

Threat Grid ユーザは、プライベートサンプルを Threat Grid アプライアンスに送信することもできます。この場合、サンプルの送信者と同じ組織に属する他の Threat Grid アプライアンスユーザと統合のユーザのみに表示されます。

次の表で、Threat Grid アプライアンスでのプライバシーおよびサンプルの可視性モデルについて説明します。

図 *1 : Threat Grid* アプライアンスでのプライバシーと可視性

Sample and Analysis Results are visible to:	Public Submissions (Default)	Private Submissions	CSA Integration Submissions (Public by Default)
Users from the Same Organization	✔	✔	✔
Users from a Different Organization	✔	✔	✔
CSA Integrations from the Same Organization	✔	✔	✔
CSA Integrations from a Different Organization	✔	✖	✔

- **フルアクセス**：緑色のチェックマークは、ユーザがサンプルと分析結果にフルアクセスできることを示します。
- **スクラビングレポート**：灰色のチェックマークは、プライベート送信の結果がスクラビングされたことを示します。ユーザはサンプルと分析結果への部分的なアクセス権を持っていますが、サンプルに関する潜在的な機密情報はすべて削除されます。Glovebox には、ファイル名、プロセス名、スクリーンショット、またはアクティビティについての詳細情報は表示されません。

  サンプルの送信者のログイン情報などの詳細情報を [Metadata] セクションから除外します。ビジネスの過程でプライベートサンプルからハッシュが発生した場合、既知の脅威に対する警告が表示されます。さらに詳細な情報が必要な場合は、完全な分析のためにサンプルの独自のコピーを送信します。

  プライベートサンプルはダウンロードされない場合があります。スクラビングレポートには、アーティファクト（ファイル名が削除されたもの）、動作インジケータ、ドメイン、IP が含まれます。

- **アクセスなし**：赤色のXは、ユーザがサンプルまたは分析結果にアクセスできないことを示します。

AMP for Endpoints プライベートクラウドと Threat Grid アプライアンスの統合には、同じ基本的なプライバシールールが適用されます。