ログ転送の概要

セキュリティイベントとトラフィックログ

セキュリティ情報イベント管理（SIEM）システムは、セキュリティ情報とセキュリティイベント情報を単一の管理プラットフォームに統合することに特化したソリューションです。セキュリティおよびイベント情報は、この情報を SIEM に転送するように設定されたサードパーティのセキュリティソリューションから発信されます。

Multicloud Defense は、セキュリティイベント情報の UI 内での直接表示をサポートしています。これらのイベントは、**[調査（Investigate）]** > **[フロー分析（Flow Analytics）]**セクションで確認できます。イベントは次のように分類され、表示できます。

カテゴリ	タイプ	説明
フローログ	FLOW_LOG	トラフィックフローのさまざまな段階に関連する情報

カテゴリ	タイプ	説明
ファイアウォールイベント	APPID	アプリケーション ID（OpenAppID）に基づいて一致したトラフィック
	GEOIP	Geo IP を発信元または宛先とするトラフィック（MaxMind）
	L4_FW	レイヤ 4 情報（送信元/宛先 IP/ポートおよびプロトコル）に基づいて一致したトラフィック
	MALICIOUS_IP	悪意のある IP（Trustwave）を発信元または宛先とするトラフィック
	SNI	SNI 情報に基づいて一致したトラフィック
ネットワーク脅威	AV	ウイルスが検出されたトラフィック（ClamAV）
	DPI	IDS/IPS 脅威が検出されたトラフィック（TALOS）
	DLP	機密データが漏えいしているトラフィック
Web の保護	WAF	Web アプリケーションの脅威が検出されたトラフィック（ModSecurity）
	L7DOS	レイヤ 7 DOS 攻撃に寄与しているトラフィック
URL フィルタリング	URLFILTER	URL カテゴリまたは URL に一致するトラフィック（Talos）
FQDN フィルタリング	FQDNFILTER	FQDN カテゴリまたは FQDN に一致するトラフィック（Talos）
HTTPS ログ	HTTP_REQUEST	Web ベースのトラフィック（HTTP）に関連する情報
	TLS_ERROR	TLS エラーに関する情報
	TLS_LOG	TLS の動作に関する情報

カテゴリ	タイプ	説明
トラフィックの概要ログ	SESSION_SUMMARY	処理された各トラフィックセッションの概要情報

（注） フローログは、ゲートウェイリリース2.10以降で廃止されました。各フローログに含まれていた情報は、**[トラフィックの概要（Traffic Summary）]** > **[ログ（Logs）]**で入手可能なセッション情報の一部として確認できます。

各イベントカテゴリは、ログ転送プロファイルを使用して SIEM に送信できます。Multicloud Defense で現在サポートされている SIEM は次のとおりです。

- AWS S3 バケット
- Datadog
- GCP ロギング
- Microsoft Sentinel
- スプランク
- Sumo Logic
- Syslog
- ウェブフック

ログ転送プロファイルは、次に概要を示す手順を使用して操作できます。

スタンドアロンイベントまたはトラフィック ログ プロファイルの作成

手順

ステップ 1 **[管理（Manage）]** > **[プロファイル（Profiles）]** > **[ログ転送（Log Forwarding）]**に移動します。
ステップ 2 [作成（Create）] をクリックします。
ステップ 3 プロファイル名と説明を入力します。
ステップ 4 [タイプ（Type）] に [スタンドアロン（Standalone）] を指定します。
ステップ 5 適切なパラメータを入力します（SIEM 固有のマニュアルを参照）。
ステップ 6 [保存（Save）] をクリックします。

ステップ 7 目的のゲートウェイの関連付けを追加します（「イベント、トラフィックログ転送プロファイル、またはメトリック転送プロファイルのゲートウェイへの追加」を参照）。

スタンドアロンイベントまたはトラフィック ログ プロファイルの編集

手順

ステップ 1 **[管理（Manage）]** > **[プロファイル（Profiles）]** > **[ログ転送（Log Forwarding）]**に移動します。
ステップ 2 編集するプロファイルの横にあるチェックボックスをオンにします。
ステップ 3 [編集（Edit）] をクリックします。
ステップ 4 必要に応じてパラメータを変更します（SIEM 固有のマニュアルを参照）。
ステップ 5 [保存（Save）] をクリックします。

グループイベントまたはトラフィック ログ プロファイルの作成

手順

ステップ 1 **[管理（Manage）]** > **[プロファイル（Profiles）]** > **[ログ転送（Log Forwarding）]**に移動します。
ステップ 2 [作成（Create）] をクリックします。
ステップ 3 プロファイル名と説明を入力します。
ステップ 4 [タイプ（Type）] に [グループ（Group）] を指定します。
ステップ 5 グループ化するスタンドアロンプロファイルの数にあわせて、必要な数の行を追加します。
ステップ 6 [保存（Save）] をクリックします。
ステップ 7 目的の**ゲートウェイの関連付け**を追加します（「イベント、トラフィックログ転送プロファイル、またはメトリック転送プロファイルのゲートウェイへの追加」を参照）。

グループイベントまたはトラフィック ログ プロファイルの編集

手順

ステップ 1 **[管理（Manage）]** > **[プロファイル（Profiles）]** > **[ログ転送（Log Forwarding）]**に移動します。

ステップ 2 編集するプロファイルの横にあるチェックボックスをオンにします。
ステップ 3 [編集（Edit）] をクリックします。
ステップ 4 スタンドアロンプロファイルを変更、追加、または削除します。
ステップ 5 [保存（Save）] をクリックします。

イベントまたはトラフィックログ転送プロファイルの表示

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [ログ転送（Log Forwarding）]**に移動します。
ステップ 2 詳細を表示するプロファイルのリンクを選択します。
ステップ 3 詳細情報を表示します。

イベントまたはトラフィック ログ プロファイルの削除

ダッシュボードからプロファイルを削除するには、次の手順を実行します。

始める前に

ダッシュボードからプロファイルを削除する前に、イベントまたはプロファイルとゲートウェイの関連付けを削除する**必要があります**。詳細については、ゲートウェイからのイベント、トラフィックログ転送プロファイル、またはメトリック転送プロファイルの削除を参照してください。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [ログ転送（Log Forwarding）]**に移動します。
ステップ 2 削除するプロファイルの横にあるチェックボックスをオンにします。
ステップ 3 [削除（Delete）] をクリックします。
ステップ 4 [はい（Yes）] または [いいえ（No）] をクリックして、削除操作を確認します。

検出ログ

検出ログは、セキュリティ情報イベント管理（SIEM）システムに転送され、単一の管理プラットフォームに集約される場合があります。

Multicloud Defense は、セキュリティイベント情報の UI 内での直接表示をサポートしています。これらのイベントは、**[調査（Investigate）]** > **[トラフィック（Traffic）]**セクションで確認できます。イベントは次のように分類され、表示できます。

カテゴリ	タイプ	説明
DNS ログ	DNS_LOG	クラウドプロバイダーから収集された DNS ログ情報と脅威インテリジェンスの相関
VPC ログ	VPC_LOG	クラウドプロバイダーから収集された VPC/VNet フローログ情報と脅威インテリジェンスの相関

各カテゴリは、ログ転送プロファイルを使用して SIEM に送信し、オンボーディングされたクラウドアカウントにプロファイルをアタッチできます。Multicloud Defense で現在サポートされているログ転送先は次のとおりです。

- AWS S3 バケット
- Datadog
- GCP ロギング
- Microsoft Sentinel
- スプランク
- Sumo Logic
- Syslog

検出ログを転送するには、次の手順を実行します。

スタンドアロン検出ログプロファイルの作成

手順

ステップ 1 **[管理（Manage）]** > **[プロファイル（Profiles）]** > **[ログ転送（Log Forwarding）]**に移動します。
ステップ 2 [作成（Create）] をクリックします。
ステップ 3 プロファイル名と説明を入力します。
ステップ 4 [タイプ（Type）] に [スタンドアロン（Standalone）] を指定します。
ステップ 5 適切なパラメータを入力します（SIEM 固有のマニュアルを参照）。
ステップ 6 [保存（Save）] をクリックします。

ステップ 7 ログプロファイルを対象のクラウドアカウントに関連付けます（「検出ログプロファイルとクラウドアカウントの追加」を参照）。

スタンドアロン検出ログプロファイルの編集

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [ログ転送（Log Forwarding）]**に移動します。
ステップ 2 編集するプロファイルの横にあるチェックボックスをオンにします。
ステップ 3 [編集（Edit）] をクリックします。
ステップ 4 必要に応じてパラメータを変更します（SIEM 固有のマニュアルを参照）。
ステップ 5 [保存（Save）] をクリックします。

グループ検出ログプロファイルの作成

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [ログ転送（Log Forwarding）]**に移動します。
ステップ 2 [作成（Create）] をクリックします。
ステップ 3 プロファイル名と説明を入力します。
ステップ 4 [タイプ（Type）] に [グループ（Group）] を指定します。
ステップ 5 行を追加して、スタンドアロンプロファイルを関連付けます。
ステップ 6 [保存（Save）] をクリックします。
ステップ 7 目的のゲートウェイの関連付けを追加します（「イベント、トラフィックログ転送プロファイル、またはメトリック転送プロファイルのゲートウェイへの追加」を参照）。

グループ検出ログプロファイルの編集

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [ログ転送（Log Forwarding）]**に移動します。
ステップ 2 編集するプロファイルの横にあるチェックボックスをオンにします。

ステップ 3 [編集（Edit）] をクリックします。
ステップ 4 スタンドアロンプロファイルを変更、追加、または削除します。
ステップ 5 [保存（Save）] をクリックします。

検出ログプロファイルの詳細の表示

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [ログ転送（Log Forwarding）]**に移動します。
ステップ 2 詳細を表示するプロファイルのリンクを選択します。
ステップ 3 詳細情報を表示します。

検出ログプロファイルとクラウドアカウントの追加

手順

ステップ 1 **[管理（Manage）] > [クラウドアカウント（Cloud Accounts）] > [アカウント（Accounts）]**に移動します。
ステップ 2 プロファイルを関連付けるクラウドアカウントの横にあるチェックボックスをオンにします。
ステップ 3 **[アクション（Actions）] > [ログプロファイルの更新（Update Log Profile）]**をクリックします。
ステップ 4 クラウドログ転送プロファイルの [ログプロファイル（Log Profile）] オブジェクトを選択します。
ステップ 5 [保存して続行（Save & Continue）] をクリックします。

クラウドアカウントからの検出ログプロファイルの削除

手順

ステップ 1 **[管理（Manage）] > [クラウドアカウント（Cloud Accounts）] > [アカウント（Accounts）]**に移動します。
ステップ 2 プロファイルの関連付けを解除するクラウドアカウントの横にあるチェックボックスをオンにします。
ステップ 3 **[アクション（Actions）] > [ログプロファイルの更新（Update Log Profile）]**をクリックします。
ステップ 4 [クラウドログ転送プロファイル（Cloud Logs Forwarding Profile）] パラメータで、[プロファイル（Profile）] の横にある [X] をクリックして削除します。

ステップ 5 [保存して続行（Save & Continue）] をクリックします。

検出ログプロファイルの削除

ダッシュボードからプロファイルを削除するには、次の手順を実行します。

始める前に

ダッシュボードからプロファイルを削除する前に、プロファイルとゲートウェイの関連付けを削除する**必要があります**。詳細については、クラウドアカウントからの検出ログプロファイルの削除を参照してください。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [ログ転送（Log Forwarding）]**に移動します。
ステップ 2 削除するプロファイルの横にあるチェックボックスをオンにします。
ステップ 3 [削除（Delete）] をクリックします。
ステップ 4 [はい（Yes）] または [いいえ（No）] をクリックして、削除操作を確認します。

ゲートウェイメトリック転送プロファイル

このプロファイルは、データのモニタリングと分析のために Multicloud Defense Gateway によって生成されたゲートウェイメトリックを転送することを目的としています。メトリックはゲートウェイによって生成されますが、メトリックをサードパーティの分析アプリケーションに転送するのは Multicloud Defense Controller です。この転送プロファイルを使用すると、Multicloud Defense にログインせずにゲートウェイメトリックをモニター、分析、および整理できます。この情報を使用してゲートウェイ環境のパフォーマンスと動作を評価できます。この情報は環境のトラブルシューティングにも利用できます。

（注） Multicloud Defense Controller バージョン 23.09 の時点では、Datadog のみがサードパーティ分析アプリケーションとしてサポートされています。

Datadog をはじめとする使用可能な分析アプリケーションのほとんどで、ツールの API とレンダリングされたデータにアクセスするには承認ユーザーである必要があります。

スタンドアロンメトリック転送プロファイルの作成

スタンドアロンプロファイルを作成し、メトリックを転送してサードパーティによって処理されるようにするには、次の手順を実行します。

始める前に

このプロファイルを作成する前に、メトリックの転送先となるサードパーティアプリケーションを少なくとも 1 つ用意してください。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [メトリック転送（Metrics Forwarding）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）] に一意のプロファイル名を入力します。

ステップ 4 （任意）[説明（Description）]に説明を入力します。これは、同様の名前を持つ他のプロファイルと区別する場合に役立ちます。

ステップ 5 [タイプ（Type）] ドロップダウンメニューを展開し、[スタンドアロン（Standalone）] を選択します。

ステップ 6 [宛先（Destination）] ドロップダウンメニューを展開し、メトリックを処理して分析するサードパーティアプリケーションを選択します。

ステップ 7 [エンドポイント（Endpoint）]に、メトリックのエンドポイントの場所として使用するエンドポイントを入力します。

ステップ 8 [保存（Save）] をクリックします。

分析アプリケーションとして Datadog を選択した場合、[エンドポイント（Endpoint）] にはデフォルトで HTTPS ウェブフックが入力されます。この入力は、デフォルトで設定されている場合、プロファイルを保存する前に変更できます。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

スタンドアロンメトリック転送プロファイルの編集

すでに作成されているスタンドアロンプロファイルを編集するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）]** > **[プロファイル（Profiles）]**に移動し、適切なプロファイルの [タイプ（Type）] を選択します。

ステップ 2 編集するプロファイルの横にあるチェックボックスをオンにします。

ステップ 3 [編集（Edit）] をクリックします。

ステップ 4 必要に応じてパラメータを変更します。

ステップ 5 [保存（Save）] をクリックします。

グループメトリック転送プロファイルの作成

このプロセスでは、プロファイルを作成し、そのプロファイルを特定のゲートウェイに割り当てます。グループプロファイルは、最大5つのスタンドアロンメトリック転送プロファイルを組み合わせたもので、単一のゲートウェイに割り当てることができます。グループ化したメトリック転送プロファイルを作成するには、次の手順を実行します。

始める前に

- このプロファイルを作成する前に、メトリックの転送先となるサードパーティアプリケーションを少なくとも 1 つ用意してください。
- 少なくとも2つのスタンドアロンメトリック転送プロファイルを作成しておく必要があります。詳細については、スタンドアロンメトリック転送プロファイルの作成を参照してください。

手順

ステップ 1 Multicloud Defense Controller インターフェイスで、**[管理（Manage）]** > **[プロファイル（Profiles）]** > **[メトリック転送（Metrics Forwarding）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）] に一意のプロファイル名を入力します。

ステップ 4 （任意）[説明（Description）] に説明を入力します。これは、似た名前のプロファイルを区別するのに役立ちます。

ステップ 5 [タイプ（Type）] ドロップダウンメニューを展開し、[グループ（Group）] を選択します。

ステップ 6 [グループの詳細（Group Details）] で、プロファイルに追加する必要がある新しい行ごとに [追加（Add）] をクリックします。

ステップ 7 各行のドロップダウンメニューを展開して、グループに追加するプロファイルを選択します。保存する前に、任意の時点でプロファイルを削除する場合は、プロファイルのチェックボックスをオンにして強調表示してから、[削除（Remove）] を選択します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

グループプロファイルの編集

すでに作成されているグループ化されたプロファイルのセットを編集するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）]**に移動し、適切なプロファイルの [タイプ（Type）] を選択します。

ステップ 2 編集するプロファイルの横にあるチェックボックスをオンにします。

ステップ 3 [編集（Edit）] をクリックします。

ステップ 4 グループプロファイルを変更、追加、または削除します。

ステップ 5 [保存（Save）] をクリックします。

プロファイルの削除

ダッシュボードからプロファイルを削除するには、次の手順を実行します。

始める前に

ダッシュボードからプロファイルを削除する前に、プロファイルとゲートウェイの関連付けを削除する**必要があります**。詳細については、ゲートウェイからのイベント、トラフィックログ転送プロファイル、またはメトリック転送プロファイルの削除を参照してください。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）]**に移動し、適切なプロファイルの [タイプ（Type）] を選択します。

ステップ 2 削除するプロファイルの横にあるチェックボックスをオンにします。

ステップ 3 [削除（Delete）] をクリックします。
ステップ 4 [はい（Yes）] または [いいえ（No）] をクリックして、削除アクションを確認またはキャンセルします。

イベント、トラフィックログ転送プロファイル、またはメトリック転送プロファイルのゲートウェイへの追加

手順

ステップ 1 **[管理（Manage）] > [ゲートウェイ（Gateways）]**に移動します。
ステップ 2 プロファイルを関連付けるゲートウェイの横にあるチェックボックスをオンにします。
ステップ 3 [編集（Edit）] をクリックします。
ステップ 4 [ログプロファイル（Log Profile）] パラメータで、メニューから目的の [プロファイル（Profile）] を選択します。
ステップ 5 [保存（Save）] をクリックします。

ゲートウェイからのイベント、トラフィックログ転送プロファイル、またはメトリック転送プロファイルの削除

手順

ステップ 1 **[管理（Manage）] > [ゲートウェイ（Gateways）]**に移動します。
ステップ 2 プロファイルの関連付けを解除するゲートウェイの横にあるチェックボックスをオンにします。
ステップ 3 [編集（Edit）] をクリックします。
ステップ 4 [ログプロファイル（Log Profile）] パラメータで、[プロファイル（Profile）] の横にある [X] をクリックして削除します。
ステップ 5 [保存（Save）] をクリックします。

（注）
ログ転送プロファイルは、ゲートウェイの作成時にゲートウェイに関連付けることもできます。[ログプロファイル（Log Profile）]パラメータは、ゲートウェイの作成プロセス中に使用できます。ここではメニューから目的の [プロファイル（Profile）] を選択できます。

ゲートウェイからのイベント、トラフィックログ転送プロファイル、またはメトリック転送プロファイルの削除

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。