ログ転送先/SIEM

AWS S3 バケット

Multicloud Defense は、AWS S3 バケットへのセキュリティイベントとトラフィックログの転送をサポートし、処理、保存、アクセス、および相関のためにセキュリティイベントとトラフィックログ情報を送信します。送信される情報は、属性と値のペアにアクセスして処理できる半構造化 JSON フォーマットとなります。

要件

イベント/ログを AWS S3 バケットに転送するには、以下が必要です。

1. 新しい AWS S3 バケットを作成するか、既存の AWS S3 バケットを使用します。
2. 次のポリシーを AWS S3 バケットに適用して、Multicloud Defense Controller によるバケットへのアクセスおよび書き込みを許可します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "<controller-role-arn>"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::<s3bucketname>/*",
```

```
            "arn:aws:s3:::<s3bucketname>"
          ]
        }
      ]
    }
```

プロファイル パラメータ

パラメータ	要件	デフォルト	説明
プロファイル名（Profile Name）	必須		プロファイルを参照するために使用する一意の名前。
説明	任意		プロファイルの説明。
接続先（Destination）	必須	AWS S3	AWS S3 バケット。
CSP アカウント（CSP Account）	必須		AWS S3 バケットが存在する CSPアカウント。
S3 バケット	必須		イベント/ログが転送される AWS S3 バケット名。

Datadog

Datadog は、多くの企業で使用されている非常に一般的で強力な SIEM です。Multicloud Defense は、Datadog へのログ転送をサポートし、処理、保存、アクセス、および関連付けのためにセキュリティイベントとトラフィックログ情報を送信します。送信される情報は、属性と値のペアにアクセスして処理できる半構造化 JSON フォーマットとなります。

要件

ログを Datadog に転送するには、次の情報が必要です。

- Datadog アカウント
- エンドポイント URL（Endpoint URL）
- API Key

ヒント

- Datadog アカウントにサインアップするには、**Datadog アカウント**（https://www.datadoghq.com/）を参照してください。
- Datadog API キーを作成するには、**Datadog API キー**（https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api）を参照してください。

プロファイル パラメータ

パラメータ	要件	デフォルト	説明
プロファイル名（Profile Name）	必須		プロファイルを参照するために使用する一意の名前。
説明	任意		プロファイルの説明。
接続先（Destination）	必須	Datadog	プロファイルに使用される SIEM。
証明書の検証をスキップ	オプション	オフ	証明書の真正性の検証をスキップするかどうか。
API Key	必須		通信を認証するための Datadog API キー。
エンドポイント	必須	https://http-intake.logs.datadoghq.com/	転送されたイベント/ログを受信するために使用される URL エンドポイント。

GCP ロギング

GCP Stackdriver Logging は、アプリケーションやサービスからログを収集して保存するための Google Cloud Provider（GCP）が提供するサービスです。Multicloud Defense は GCP Stackdriver Logging へのログ転送をサポートし、処理、ストレージ、アクセス、および相関用にセキュリティイベントとトラフィックログ情報を送信します。送信される情報は、属性と値のペアにアクセスして処理できる半構造化 JSON フォーマットとなります。

要件

ゲートウェイが GCP Stackdriver Log にイベントを書き込むには、GCP *Multicloud Defense-firewall* サービスアカウントに [ログ作成者（Logs Writer）] ロールを割り当てる必要があります。

プロファイル パラメータ

パラメータ	要件	デフォルト	説明
プロファイル名（Profile Name）	必須		プロファイルを参照するために使用する一意の名前。
説明	任意		プロファイルの説明。
接続先（Destination）	必須	GCP ロギング（ゲートウェイから）	プロファイルに使用される SIEM。
ログ名（Log Name）	必須	ciscomcd -gateway-logs	イベントを保存するために使用される Stackdriver Log の名前。

フィールドの整数から文字列へのマッピング

イベントがコントローラから転送されると、コントローラはイベントフィールド値のフレンドリ名へのマッピングを導入します。イベントがゲートウェイから直接転送される場合（GCP ロギングなど）、コントローラは関与しないため、イベントフィールド値はフレンドリ名にマッピングされません。これらのフィールドを解釈するには、ユーザーは、フィールド値からフレンドリ名へのマッピングを実行する必要があります。

フレンドリにマッピングされるフィールド、サブフィールド、およびそれらの値を以下に示します。

フィールド	整数	文字列
action	[0]	DUMMY_ACTION
	1	ALLOW
	2	拒否
	3	DROP
	4	REDIRECT
	5	PROXY
	6	LOG
	7	OTHER
	8	DELAY
	9	DETECT_SIG

フィールド	整数	文字列
gatewaySecurityType	1	INGRESS_FIREWALL
	2	EAST_WEST_AND_EGRESS_FIREWALL

フィールド	整数	文字列
level	1	DEBUG
	2	INFO
	3	NOTICE
	4	WARNING
	5	ERROR
	6	重大
	7	ALERT
	8	EMERGENCY

フィールド	整数	文字列
policyMatchInfo.serviceType	[0]	UNKNOWN
	1	PROXY
	2	FORWARDING
	3	REVERSE_PROXY
	4	FORWARD_PROXY

フィールド	整数	文字列
protocol **sessionSummaryInfo.egressConnection.protocol** **sessionSummaryInfo.ingressConnect.protocol**	[0]	DUMMY
	1	ICMP
	6	TCP
	17	UDP
	252	HTTP

フィールド	整数	文字列
rule.type	[0]	DUMMY_RULE_TYPE
	1	THIRD_PARTY
	2	USER_DEFINED

フィールド	整数	文字列
statusText **ingressConnectionStates.state**	0	CLOSED
	1	SYN_SENT
	2	SYN_RECV
	3	ESTABLISHED
	4	FIN_WAIT
	5	CLOSE_WAIT
	6	LAST_ACK
	7	TIME_WAIT
	8	CLOSE

フィールド	整数	文字列
type	1	WAF
	2	DPI
	3	HTTP_REQUEST
	4	L4_FW
	5	FLOW_LOG
	6	MALICIOUS_IP
	7	TLS_ERROR
	8	TLS_LOG
	9	L7DOS
	10	SNI
	11	APPID
	12	URLFILTER
	13	SESSION_SUMMARY
	14	DLP
	15	FQDNFILTER
	16	AV

Microsoft Sentinel

Microsoft Sentinel は、多くの企業で使用されている非常に一般的で強力な SIEM です。Multicloud Defense は、Microsoft Sentinel へのログ転送をサポートし、処理、保存、アクセス、および関連付けのためにセキュリティイベントとトラフィックログ情報を送信します。送信される情報は、属性と値のペアにアクセスして処理できる半構造化 JSON フォーマットとなります。

要件

ログを Microsoft Sentinel に転送するには、次の情報が必要です。

- Azure ログ分析ワークスペースを作成します。
- Azure ログテーブルを定義します。

プロファイル パラメータ

パラメータ	要件	デフォルト	説明
プロファイル名（Profile Name）	必須		プロファイルを参照するために使用する一意の名前。
説明	任意		プロファイルの説明。
接続先（Destination）	必須	Microsoft Sentinel	プロファイルに使用される SIEM。
Azure ログ分析ワークスペース ID（Azure Log Analytics Workspace ID）	必須		Azure ログ分析ワークスペースの ID。
共有キー	必須		通信の認証に使用される共有キー。
Azure ログテーブル名（Azure Log Table Name）	必須		ログ/イベントが保存される Azure ログテーブルの名前。

スプランク

Splunk は、多くの企業で使用されている非常に一般的で強力な SIEM です。Multicloud Defense は、Splunk へのログ転送をサポートし、処理、保存、アクセス、および関連付けのためにセキュリティイベントとトラフィックログ情報を送信します。送信される情報は、属性と値のペアにアクセスして処理できる半構造化 JSON フォーマットとなります。

要件

ログを Splunk に転送するには、次の情報が必要です。

- Splunk アカウント
- Splunk コレクタ URL
- イベントコレクタキー
- インデックス名

ヒント　Splunk イベントコレクタの詳細については、『**Splunk HTTP イベントコレクタ**』（https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/UsetheHTTPEventCollector）を参照してください。

プロファイル パラメータ

パラメータ	要件	デフォルト	説明
プロファイル名（Profile Name）	必須		プロファイルを参照するために使用する一意の名前。
説明	任意		プロファイルの説明。
接続先（Destination）	必須	Datadog	プロファイルに使用される SIEM。
証明書の検証をスキップ	オプション	オフ	証明書の真正性の検証をスキップするかどうか。
エンドポイント	必須		HTTP イベントコレクタへのアクセスに使用される URL。
トークン	必須		Multicloud Defense が Splunk と通信できるようにする Splunk トークン。
索引	必須	メイン（main）	イベントの保存に使用される Splunk インデックスの名前。

Sumo Logic

Sumo Logic は、多くの企業で使用されている非常に一般的で強力な SIEM です。Multicloud Defense は、Sumo Logic へのログ転送をサポートし、処理、保存、アクセス、および関連付けのためにセキュリティイベントとトラフィックログ情報を送信します。送信される情報は、属性と値のペアにアクセスして処理できる半構造化 JSON フォーマットとなります。

要件

ログを Sumo Logic に転送するには、次の情報が必要です。

- Sumo Logic アカウント
- Sumo Logic コレクタエンドポイント

ヒント Sumo Logic コレクタのセットアップ方法については、『**Sumo Logic セットアップガイド**』（https://help.sumologic.com/docs/send-data/setup-wizard/）を参照してください。

プロファイル パラメータ

パラメータ	要件	デフォルト	説明
プロファイル名（Profile Name）	必須		プロファイルを参照するために使用する一意の名前
説明	任意		プロファイルの説明
接続先（Destination）	必須	Sumo Logic	プロファイルに使用される SIEM
エンドポイント	必須		転送されたイベント/ログを受信するために使用される URL エンドポイント

Syslogs

syslog サーバーは、標準形式の syslog メッセージを受け入れる一般的なログコレクタです。各 syslog メッセージには、ファシリティ、重大度、およびメッセージのフィールドが含まれています。ほぼすべての SIEM は syslog 形式のメッセージを受け入れることができますが、大部分の SIEM は他のメッセージ形式をサポートしています。Multicloud Defense は、syslog サーバーへのセキュリティイベントとトラフィックログの送信をサポートします。転送されるイベントとログのリストを次に示します。

- フローログ（トラフィックの概要）
- ファイアウォールイベント（AppID、L4FW、GeoIP、MaliciousIP、SNI）
- HTTPS ログ（HTTP、 TLS）
- ネットワークの脅威（AV、DLP、IDS/IPS）
- Web 保護（WAF、L7 DoS）

現時点では、このリストに記載されているイベントとログは必須であり、変更できません。syslog を転送するように設定すると、これら**すべて**のログがレポートに含まれます。

（注） フローログは、ゲートウェイバージョン2.10以降のリリースで廃止されました。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。

イベントは、ログ転送プロファイルを使用して syslog サーバーに転送できます。イベントを syslog サーバーに送信するには、作成されたプロファイルを新規または既存のゲートウェイに関連付ける必要があります。ログ転送プロファイルとゲートウェイの関連付けを作成、修正、または変更するには、「ログ転送：セキュリティイベントとトラフィックログ」を参照してください。

プロファイル パラメータ

パラメータ	要件	デフォルト	説明
プロファイル名（Profile Name）	必須		プロファイルを参照するために使用する一意の名前。
説明	任意		プロファイルの説明。
SIEM ベンダー	必須	Syslog	プロファイルに使用される SIEM。
サーバー IP（Server IP）	必須		syslog サーバの IP アドレス。
プロトコル	必須	UDP	メッセージの送信時に使用するプロトコル（TCP/UDP）。
ポート	必須		メッセージの送信時に使用するポート。
書式	必須	IETF	メッセージの形式（IETF のみがサポートされます）。
フローログ	必須	非対応	フローログを送信するかどうか（Yes/No）。
ファイアウォールイベント	必須	非対応	ファイアウォールイベントを送信するかどうか（Yes/No）。
HTTPS ログ	必須	非対応	HTTPS ログを送信するかどうか（Yes/No）。

パラメータ	要件	デフォルト	説明
ネットワーク脅威	必須	Emergency	ネットワーク脅威を送信する最も低い重大度レベル。
Web 攻撃	必須	Emergency	Web 攻撃を送信する最も低い重大度レベル。

（注） 次の重大度レベル（最も高いものから順に示す）を使用できます。

- 緊急（Emergency）
- [アラート（Alert）]
- 重大（Critical）
- [エラー（Error）]
- 警告
- [通知（Notice）]
- 情報
- デバッグ

指定した重大度レベル以上が含まれるカテゴリのすべてのイベントがsyslogサーバーに送信されます。

Webhook

ウェブフックを使用したログ転送は、さまざまなシナリオで有益なプラクティスであり、特に異なるシステムやサービスをリアルタイムで統合する必要がある場合に便利です。ウェブフックは、リアルタイムのデータ転送を可能にし、イベント駆動型アーキテクチャまたは集中型ロギングに最適であるだけでなく、自動化や他のサードパーティサービスとの統合もサポートします。特定の環境をサポートするようにログ転送プロファイルをカスタマイズできます。

要件

認証トークンまたはパスワードを必要とするサービスにログを転送する場合は、あらかじめ認証トークンまたはパスワードを設定しておき、このプロファイルを作成するときにすぐに使用できるようにします。

プロファイル パラメータ

パラメータ	要件	デフォルト	説明
プロファイル名（Profile Name）	必須		プロファイルを参照するために使用する一意の名前。
説明	任意		プロファイルの説明。
タイプ	必須		[スタンドアロン（Standalone）] を選択します。
接続先（Destination）	必須	Webhook	
エンドポイント	必須		ウェブフックの URL を入力します。
メッセージフィールド名	必須		この値は、送信されるデータの構造と意味を定義します。
バッチサイズ（Batch size）	必須	100	この値は、1 回の伝送でまとめて送信するログエントリの数を決定します。
認証タイプ	必須		ユーザー名とパスワード、または**ベアラートークン**に [基本（Basic）] を選択します。

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。