Log Forwarding Overview

Security Events and Traffic Logs

Security Information Event Management (SIEM) systems are solutions that specialize in combining security information and security event information together into a single management platform. The security and event information will originate from 3rd party security solutions that are configured to forward this information to the SIEM.

Multicloud Defense supports viewing security event information directly within the UI. These events are available under the **Investigate** > **Flow Analytics** section. The events are categorized and viewable as follows:

Category	Type	Description
Flow Logs	FLOW_LOG	Information related to the different stages of a traffic flow
Firewall Events	APPID	Traffic matched based on Application ID (OpenAppID)
	GEOIP	Traffic sourced from or destined to a Geo IP (MaxMind)
	L4_FW	Traffic matched based on layer4 information (Source/Dest IP/Port and Protocol)
	MALICIOUS_IP	Traffic sourced from or destined to a malicious IP (Trustwave)
	SNI	Traffic matched based on SNI information

Category	Type	Description
Network Threats	AV	Traffic where a virus has been detected (ClamAV)
	DPI	Traffic where an IDS/IPS threat has been detected (TALOS)
	DLP	Traffic where sensitive data is being exfiltration
Web Protection	WAF	Traffic where a web application threat has been detected (ModSecurity)
	L7DOS	Traffic that is contributing to a layer7 DOS attack
URL Filtering	URLFILTER	Traffic that matches a URL category or URL (Talos)
FQDN Filtering	FQDNFILTER	Traffic that matches a FQDN category or FQDN (Talos)
HTTPS Logs	HTTP_REQUEST	Information related to web-based traffic (HTTP)
	TLS_ERROR	Information related to TLS errors
	TLS_LOG	Information related to TLS behavior
Traffic Summary Logs	SESSION_SUMMARY	Summary information on each processed traffic session

Note Flow Logs are deprecated in 2.10 and later gateway releases. The information contained within each flow Log is made available as part of the session information available in **Traffic Summary** > **Logs**.

Each of the event categories can be sent to a SIEM using a log forwarding profile. The SIEMs currently supported by Multicloud Defense are:

- AWS S3 Bucket
- Datadog
- GCP Logging
- Microsoft Sentinel
- Splunk
- Sumo Logic
- Syslog
- Webhooks

A log forwarding profile can be operated on using the steps outlined below:

Create a Standalone Event or Traffic Log Profile

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Click **Create**.
Step 3 Specify a Profile Name and Description.
Step 4 Specify *Type* as Standalone.
Step 5 Fill in the appropriate parameters (refer to the SIEM-specific documentation).
Step 6 Click **Save**.
Step 7 Add the desired Gateway Associations (refer to Add an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile to a Gateway).

Edit a Standalone Event or Traffic Log Profile

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Check the box next to the Profile you want to *Edit*.
Step 3 Click **Edit**.
Step 4 Modify the parameters as desired (refer to the SIEM-specific documentation).
Step 5 Click **Save**.

Create a Group Event or Traffc Log Profile

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Click **Create**.
Step 3 Specify a Profile Name and Description.
Step 4 Specify *Type* as Group.
Step 5 Add as many rows as needed to accommodate for the number of standalone profiles you want to group.
Step 6 Click **Save**.

Step 7 Add the desired **gateway associations** (refer to Add an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile to a Gateway).

Edit a Group Event or Traffc Log Profile

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Check the box next to the Profile you want to *Edit*.
Step 3 Click **Edit**.
Step 4 Modify, Add or Remove Standalone Profiles.
Step 5 Click **Save**.

View an Event or Traffic Log Forwarding Profile

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Select the Profile link you want to view the *Details*.
Step 3 View the *Details* information.

Delete an Event or Traffc Log Profile

Use the following procedure to delete the profile from your dashboard:

Before you begin

You **must** remove the association between the event or profile and the gateway before you delete the profile from your dashboard. See Remove an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile from a Gateway for more information.

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Check the box next to the Profile you want to *Delete*.
Step 3 Click **Delete**.

Step 4 Confirm the *Delete* operation by clicking **Yes** or **No**.

Discovery Logs

Discovery logs may be forwarded to Security Information Event Management (SIEM) systems to aggregate into a single management platform.

Multicloud Defense supports viewing security event information directly within the UI. These events are available under the **Investigate** > **Traffic** section. The events are categorized and viewable as follows:

Category	Type	Description
DNS Logs	DNS_LOG	Correlation of Threat Intelligence with DNS Log information gathered from cloud provider
VPC Logs	VPC_LOG	Correlation of Threat Intelligence with VPC/VNet Flow Log information gathered from cloud provider

Each of the categories can be sent to a SIEM using a Log Forwarding Profile and attaching the Profile to the onboarded Cloud Account. The Log Forwarding destinations currently supported by Multicloud Defense are:

- AWS S3 Bucket
- Datadog
- GCP Logging
- Microsoft Sentinel
- Splunk
- Sumo Logic
- Syslog

To forward Discovery Logs, use the steps below:

Create a Standalone Discovery Log Profile

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Click **Create**.
Step 3 Specify a Profile Name and Description.
Step 4 Specify *Type* as Standalone.

Step 5 Fill in the appropriate parameters (refer to the SIEM-specific documentation).
Step 6 Click **Save**.
Step 7 Associate the Log Profile to the desired Cloud Accounts (refer to Add a Discovery Log Profile with a Cloud Account).

Edit a Standalone Discovery Log Profile

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Check the box next to the profile you want to *Edit*.
Step 3 Click **Edit**.
Step 4 Modify the parameters as desired (refer to the SIEM-specific documentation).
Step 5 Click **Save**.

Create a Group Discovery Log Profile

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Click **Create**.
Step 3 Specify a Profile Name and Description.
Step 4 Specify *Type* as Group.
Step 5 Add a row for to associate a Standalone Profile.
Step 6 Click **Save**.
Step 7 Add the desired Gateway Associations (refer to Add an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile to a Gateway).

Edit a Group Discovery Log Profile

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Check the box next to the Profile you want to *Edit*.
Step 3 Click **Edit**.

Step 4 Modify, Add or Remove Standalone Profiles.
Step 5 Click **Save**.

View a Discovery Log Profile Details

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Select the Profile link you want to view the *Details*.
Step 3 View the *Details* information.

Add a Discovery Log Profile with a Cloud Account

Procedure

Step 1 Navigate to **Manage** > **Cloud Accounts** > **Accounts**.
Step 2 Check the box next the cloud account you want to associate the *Profile*.
Step 3 Click **Actions** > **Update Log Profile**.
Step 4 Select the **Log Profile** object for cloud logs forwarding profile.
Step 5 Click **Save & Continue**.

Remove a Discovery Log Profile from a Cloud Account

Procedure

Step 1 Navigate to **Manage** > **Cloud Accounts** > **Accounts**.
Step 2 Check the box next the Cloud Account you want to disassociate the *Profile*.
Step 3 Click **Actions** > **Update Log Profile**.
Step 4 For the *Cloud Logs Forwarding Profile* parameter, click the 'X' next to the *Profile* to remove it.
Step 5 Click **Save & Continue**.

Delete a Discovery Log Profile

Use the following procedure to delete the profile from your dashboard:

Before you begin

You **must** remove the association between the profile and the gateway before you delete the profile from your dashboard. See Remove a Discovery Log Profile from a Cloud Account for more information.

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.

Step 2 Check the box next to the Profile you want to *Delete*.

Step 3 Click **Delete**.

Step 4 Confirm the *Delete* operation by clicking **Yes** or **No**.

Gateway Metrics Forwarding Profile

This profile is intended to forward gateway metrics generated by the Multicloud Defense Gateway for data monitoring and analysis.While the metrics are generated by the gateway, it is the Multicloud Defense Controller that forwards the metrics to the third party analysis application. With this forwarding profile you are able to monitor, analyze, and organize your gateway metrics without logging into Multicloud Defense. Use this information to gauge the performance and behavior of your gateway environment; you can also utilize this information for environmental troubleshooting.

Note As of Multicloud Defense Controller version 23.09, only Datadog is supported as a third party analytics application.

For the majority of analytics applications available, for example, Datadog, you must already be an authorized user to access the tool's APIs and rendered data.

Create a Standalone Metrics Forwarding Profile

Use the following procedure to create a standalone profile and forward metrics to be processed by a third party:

Before you begin

You must have at least one third party application to forward the metric to prior to creating this profile.

Procedure

Step 1 Navigate to **Manage** > **Profiles** > **Metrics Forwarding**.
Step 2 Click **Create**.
Step 3 Enter a unique profile **Name**.
Step 4 (Optional) Enter a **Description**. This may help differentiate from other profiles with a similar name.
Step 5 Expand the **Type** drop-down menu and select **Standalone**.
Step 6 Expand the **Destination** drop-down menu and select the third-party application to process and analyze the metrics.
Step 7 Enter the **Endpoint** to be used as the endpoint location for the metrics.
Step 8 Click **Save**.

If you select Datadog as your analyitics application, the **Endpoint** is filled in by default with an HTTPs webhook. This entry, if defaulted, can be modified prior to saving the profile.

What to do next

Attach the profile to a policy rule set. See Rule Sets and Rule Set Groups for more information.

Edit a Standalone Metrics Forwarding Profile

Use the following procedure to edit a standalone profile that has already been created.

Procedure

Step 1 Navigate to **Manage** > **Profiles** and select the appropriate profile **Type**.
Step 2 Check the box next to the profile you want to edit.
Step 3 Click **Edit**.
Step 4 Modify the parameters as desired.
Step 5 Click **Save**.

Create a Group Metrics Forwarding Profile

In this process, you create a profile and then assign it to a specific gateway. A group profile combines up to five standalone metrics forwarding profile that can then be assigned to a single gateway. Use the following procedure to create a grouped metrics forward profile:

Before you begin

- You must have at least one third party application to forward the metric to prior to creating this profile.

- You must have at least two standalone metrics forwarding profiles already created. See Create a Standalone Metrics Forwarding Profile for more information.

Procedure

Step 1 In the Multicloud Defense Controller interface navigate to **Manage** > **Profiles** > **Metrics Forwarding**.
Step 2 Click **Create**.
Step 3 Enter a unique **Profile Name**
Step 4 (Optional) Enter a **Description**. This may help differentiate between profiles with a similar name.
Step 5 Expand the **Type** drop-down menu and select **Group**.
Step 6 Under **Group Details**, click **Add** for every new row you need to add to the profile.
Step 7 Expand the drop-down menus for each row to select a profile to add to the group. If you want to remove a profile at any point prior to saving, select the profile's checkbox so it is highlighted and select **Remove**.
Step 8 Click **Save**.

What to do next

Attach the profile to a policy rule set. See Rule Sets and Rule Set Groups for more information.

Edit a Group Profile

Use the following procedure to edit a set of grouped profiles that has already been created:

Procedure

Step 1 Navigate to **Manage** > **Profiles** and select the appropriate profile **Type**.
Step 2 Check the box next to the profile you want to *Edit*.
Step 3 Click **Edit**.
Step 4 Modify, add or remove group profiles.
Step 5 Click **Save**.

Delete a Profile

Use the following procedure to delete the profile from your dashboard:

Before you begin

You **must** remove the association between the profile and the gateway before you delete the profile from your dashboard. See Remove an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile from a Gateway for more information.

Procedure

Step 1 Navigate to **Manage** > **Profiles** and select the appropriate profile **Type**.
Step 2 Check the box next to the profile you want to delete.
Step 3 Click **Delete**.
Step 4 Click **Yes** or **No** to either confirm or cancel the delete action.

Add an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile to a Gateway

Procedure

Step 1 Navigate to **Manage** > **Gateways**.
Step 2 Check the box next the gateway you want to associate the *Profile*.
Step 3 Click **Edit**.
Step 4 For the *Log Profile* parameter, select the desired *Profile* from the menu.
Step 5 Click **Save**.

Remove an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile from a Gateway

Procedure

Step 1 Navigate to **Manage** > **Gateways**.
Step 2 Check the box next the gateway you want to de-associate the *Profile*.
Step 3 Click **Edit**.
Step 4 For the *Log Profile* parameter, click the 'X' next to the *Profile* to remove it.
Step 5 Click **Save**.

Note A Log Forwarding Profile can also be associated with a gateway at time of gateway creation. The *Log Profile* parameter is available during the gateway creation process, where the desired *Profile* can be selected from the menu.