Cloud Visibility Reports

Reports provide valuable statistical information that you can use as insight to the network and its genereal health, and make decisions accordingly. Multicloud Defense provides the ability to generate the following types of reports:

Discovery

The Generate a Discovery Report is generated by taking out-of-band traffic information from DNS queries and VPC flow logs, and correlating the data with threat intelligence and cloud inventory information. These logs are only available if you configure the VPC of your cloud service provider to send logs to an S3 bucket, which are then transferred directly to the Multicloud Defense Controller.

Threat Indicators Snapshot

The Generate a Threat And Cloud Analytics Report report is a compilation of data on the gateway instance. You can use this report to determine the gateway's endurance under duress by examining traffic patterns, when and how thresholds are met, trends of attacks, and specific instances. The report includes the following points:

- **IDS/IPS Detection** - This data is how many attacks detected, the type of attack, the time of the detected attacks, and the top ten IDS/IPS signatures over the time range selected.
- **WAF Detection** - This data is how many attacks detected by WAF rule(s), the time of the detected attacks, and the top ten WAF signatures over the time range selected.
- **Gelocation of Threats by Volume** - This choropleth map that shows the volume of attacks for both WAF and IDS/IPS events by country in volume.
- **Top Ten Attacking Countries by Volume and Time** - This horizontal bar chart depicts the volume of the top 10 countries that during the entirety of the timespan produced the most events, then displayed breaking that volume across the time increments for which the events occurred during the timespan.
- **Policy and Prevention** - This data chart shows the action taken by the gateway security type in whichever CSP environment it is deployed in. This includes the type of action, how many events generated from the action, the gateway security type and more.

Note that you **must** have Web Application Firewall (WAF), intrusion detection and protention (IDS/IPS) rules enabled in your policy in order for the Multicloud Defense Gateway to collect and poll data.

For Additional Information:

- Generate a Discovery Report, on page 2

• Generate a Threat And Cloud Analytics Report, on page 2

Generate a Discovery Report

A discovery report is generated by taking DNS queries and VPC flow logs that have been sent to an S3 bucket prior to getting processed by the Multicloud Defense Controller.

Use the following procedure to generate a Discovery Report:

Step 1 In the Multicloud Defense Controller page, navigate to **Reporting**.

Step 2 Select **Discovery**.

Step 3 Click on the **Generate** button. The report is generated in a new tab.

Step 4 The report is generated. To save the report locally, click **Print Report** and navigate to where you want the report saved on your local server.

Generate a Threat And Cloud Analytics Report

The Threat and Cloud Analytics Report is a **Threat Indicator Snapshot** that is generated by using the traffic collected and inspected by Multicloud Defense Gateway. This provides a more comprehensive report as Multicloud Defense is now in the datapath and compliments the discovery report.

Note that reports cannot be generated for the day of, since a qualitative summarization of events cannot be made until end of day, end of month, end of quarter, or end of year.

Note You **must** have Web Application Firewall (WAF), intrusion detection and protection (IDS/IPS) rules enabled in your policy in order for the Multicloud Defense Gateway to collect and poll data. For more information, see the following links respecitvely:

- Web Application Firewall
- Network Intrusion (IDS/IPS) Profile

Use the following procedure to generate a Threat And Cloud Analytics with the threat indicators snapshot:

Step 1 In the Multicloud Defense Controller page, navigate to **Reporting**.

Step 2 Select **Threat Indicators Snapshot**.

Step 3 Use the drop-down menu to select the **Frequency** the data is pulled: daily, weekly, monthly, quarterly, or yearly.

- **Daily** - From 12AM for 24 hours. This is in UTC time.
- **Weekly** - From Monday to Sunday.
- **Monthly** - Generally from the beginning to the end of the month.

- **Quarterly** - From the beginning to end of a quart. Quarters are generally defined as from January 1 - March 31, April 1 - June 30, July 1 - September 30, and October 1 - December 31.
- **Yearly** - From January 1 to December 31 of the year selected.

Step 4 Use the drop-down **Calendar** to select the time range, or specific days, that you want to collect data on. Days that are grayed out have no data to compile. If you have no data available to generated a report, confirm your policies contain WAF and IDS/IPS rules.

Step 5 Click **Generate Report**.

Step 6 The report is generated. To save the report locally, click **Print Report** and navigate to where you want the report saved on your local server.