MANAGED DENIAL OF SERVICE PROTECTION CLOUD SERVICE (MSS-DDOS-CLOUD)

V053023

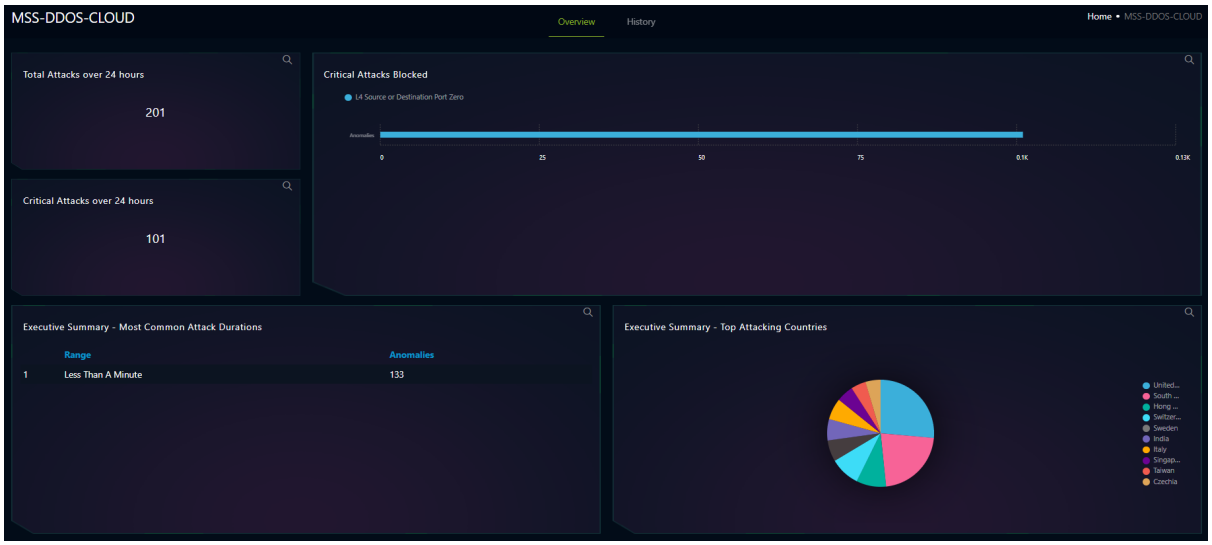
Revision V053023

This document is a briefing that describes the operation and use of the Managed Denial of Service Protection Cloud, and it is meant for all users of SKYWATCH WEB Platform.

Purpose of this Dashboard

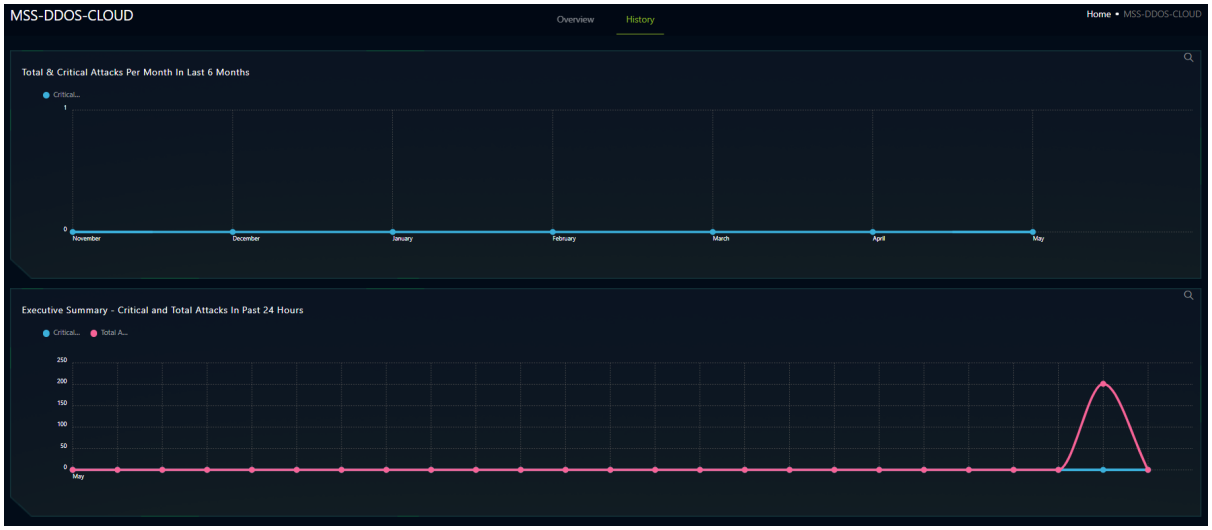
This SKYWATCH Dashboard(s) provide **visibility** to the technical and executive users of SKYWATCH for the **MSS-DDOS-CLOUD** Service and the ability to generate an on-demand **report** for this service (with the information of the dashboard). These are two of deliverables for the service. There are more consolidated reports that combine the information of this service with other contracted services. Also certain of the parameters defined on this Dashboard are used as indicators to trigger SKYWATCH automations (GLESEC NOTABLE EVENTS – GNE) and this activates the GLESEC OPERATION CENTER(s) (GOC) to further investigate and for incident-response purpose.

The following presents the SKYWATCH MSS-DDOS-CLOUD



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500



Detailed Description of functionality of the MSS-DDOS-CLOUD Dashboard

Below the description and use cases of each of the components.

ITEM	DESCRIPTION
Overview	
Total Attacks for period	Displays the # of DDOS attacks made within the last 24 hours. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to quickly determine the number of attacks that occurred in the last 24 hours.***
Critical Attacks over 24 hours	Displays the # of DDOS attacks of critical severity made within the last 24 hours. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to quickly determine the number of critical severity attacks that occurred in the last 24 hours.***
Critical Attacks Blocked	Displays a stacked horizontal bar chart that shows the critical DDOS attack signatures blocked for each category of DDOS attack. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to keep track of critical severity ddos attacks.***
Executive Summary – Most Common Attack Durations	Displays the duration of DDOS attacks by category. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to gain insight as to how long different categories of attacks are taking.***

Executive Summary – Top Attacking Countries	Displays the top 10 countries that DDOS attacks have originated from as a pie chart. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***The purpose of this table is to show more detail from what is viewed in the RADAR.***
Types of Blocked Attacks	Displays a stacked horizontal bar chart that shows the attack signatures blocked for each category. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to determine the most common blocked attack categories and how many attacks were blocked for each category.***
Top Attack Sources	Displays the # of DDOS attacks blocked for the top 10 attack sources as a horizontal bar chart. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to determine the most common sources of attacks.***
Top Assets Protected	Displays the # of DDOS attacks blocked for the top 10 most attacked destinations as a horizontal bar chart. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to determine the top attacked destinations.***
Executive Summary - Types of Blocked Attacks	Displays a pie chart showing the # of attacks for each attack category. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to compare the volume of attacks per each threat category.***
Top Attack Type Per Protected Asset	Displays a stacked horizontal bar chart showing the destinations for each attack signature. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to determine which destinations receive the most attacks of a specific attack signature.***
Top Blocked DDOS Types	Displays a stacked horizontal bar chart showing the categories of blocked DDOS attacks for each communication protocol. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to gain insight as to the most common protocols used in attacks and the attacks executed through those protocols.***
Executive Summary – Total Bandwidth/Packet Count by Type	Displays the total bandwidth of DDOS attacks for each attack category. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to monitor the bandwidth used by DDOS attacks.***

Executive Summary – Attacks Blocked by Destination Port	Displays the # of blocked DDOS attacks for every attacked port. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to determine which ports are the most likely to be hit by a DDOS attack.***
History	
Total & Critical Attacks per month in last 6 months	Displays the # of critical and total DDOS attacks made each month for the last 6 months as line graphs. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 6 months. ***This information can be used to see the change in the critical and total number of attacks every month for the last 6 months.***
Executive Summary – Critical and Total Attacks last 24 hours	Displays the # of critical and total DDOS attacks made each hour for the last 24 hours as a line graph. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to see the change in the critical and total number of attacks for every hour for the last 24 hours.***
ON-DEMAND REPORT	This action button will generate a MSS-DDOS-CLOUD REPORT based on the data of the dashboard with the corresponding TLP AMBER designation.
HOW TO USE THIS DASHBOARD	Presents this document.