GLESEC
COMPLETELY PERSPECTIVE

MANAGED WEB APPLICATION FIREWALL CLOUD PROTECTION SERVICE (MSS-WAF-CLOUD)

V053023

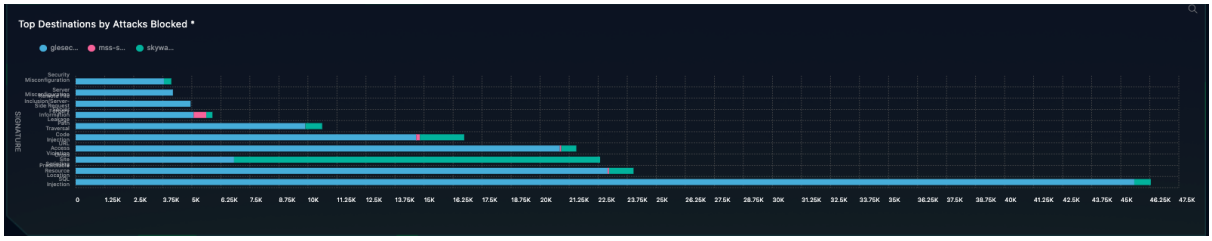
Revision V053023

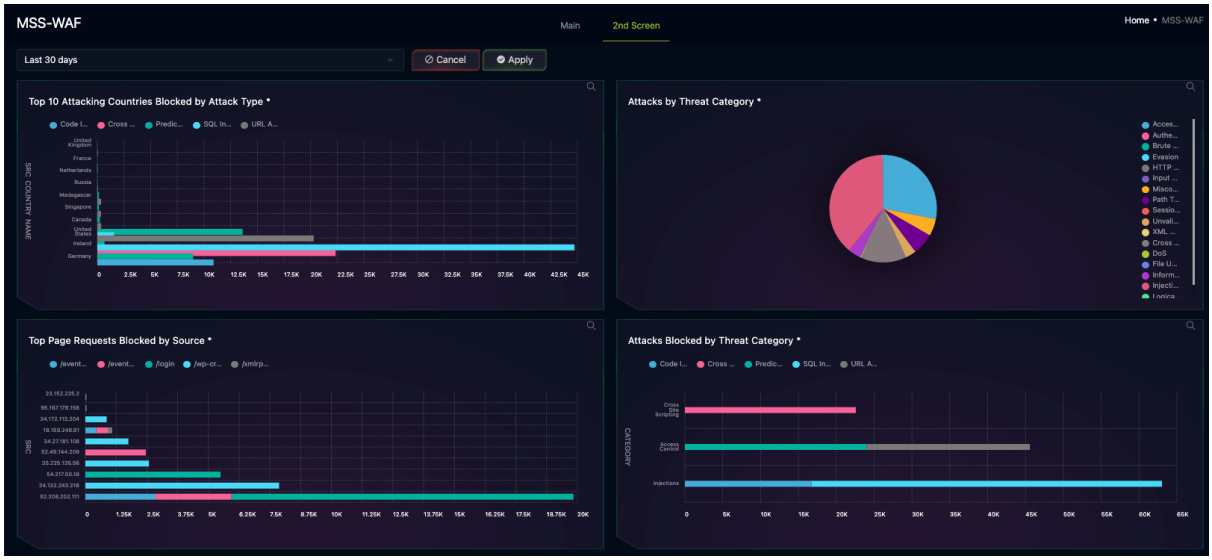
This document is a briefing that describes the operation and use of the Managed Web Application Firewall CLOUD Protection, and it is meant for all users of SKYWATCH WEB Platform.

Purpose of this Dashboard

This SKYWATCH Dashboard(s) provide **visibility** to the technical and executive users of SKYWATCH for the **MSS-WAF-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-WAF-CLOUD





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

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

ITEM	DESCRIPTION
Overview	
Blocked Events	Displays the # of events blocked by the WAF. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine the number of attacks that occurred in the last 24 hours.***
Applications	Displays the # of applications deployed on the WAF. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine the number of applications deployed on the WAF-CLOUD solution.***

Application Attack Distribution	Displays a pie chart showing the # of attacks per every action taken by the WAF. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine the distribution of attacks by the actions taken by the WAF.***
Attack Module Distribution	Displays a pie chart showing the distribution of attack modules used by the WAF. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine the distribution of attack modules used by the WAF.***
OWASP Top 10 Mapping	Displays a pie chart that maps the distribution of vulnerabilities from the OWASP top 10 list. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine where the WAF solution is focusing its protection and mitigation efforts.***
Application Security Events	Displays the # of security events detected on the WAF for each severity level for each day for the last 30 days as a line graph. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine the frequency of detected attacks at each severity level over time.***
HTTP Transactions	Displays the amount of blocked and legitimate HTTP traffic to the WAF for each day for the last 30 days as a line graph For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine the frequency of blocked and legitimate HTTP traffic on the WAF.***
Top Application Attacked Hosts	Displays a horizontal bar chart showing the top most attacked hosts and the # of attacks for each host. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine which hosts are receiving the most attacks.***
Top Application Attack Sources	Displays a horizontal bar chart showing the top attack sources and the # of attacks for each source. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine which sources are generating the most attacks.***
Top Page Requests Blocked	Displays a horizontal bar chart showing the top page requests that are blocked for each source. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours.

	This information can be used to determine which pages are most requested by a source. This can be used to help identify when the WAF is blocking legitimate traffic.
Application Attack Geomap	Displays a map that visualizes the distribution of attacks by the detected location of the attack source. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine which countries have a high volume of attacks. This can be used to help identify when a geo-blocking rule should be implemented on the WAF.***
Top Attacked Applications	Displays a horizontal bar chart showing the top attacked applications deployed on the WAF and the volume of attacks for each application. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine which applications are receiving the highest volume of attacks.***
Certificates	Displays the certificates installed on the WAF. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine the certificates installed on the WAF and how long until they expire.***
Applications	Displays the applications that are deployed on the WAF. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. ***This information can be used to quickly determine the applications that are deployed on the WAF-CLOUD solution.***
History	
Total & Critical Attacks per Month in Last 6 Months	Displays the # of total and critical attacks on the WAF. 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 check for any spikes in activity and verify a consistent level of blocked activity.***
Attack Types Blocked by Month	Displays the # of each attack that occurred for each month for the last 6 months. 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 identify spikes in activity over the course of several weeks.***
Top 10 Attacking Countries Blocked Over 6 Months	Displays the # of attack types blocked for the top 10 attacking countries blocked by the WAF. For the SKYWATCH WEB the refresh rate is once a month. The information represents data from last 6 months. ***This information can be used to determine which countries do most attacks originate from and what are the most popular attacks used by sources in those countries.***
ON-DEMAND REPORT	This action button will generate the MSS-WAF-CLOUD REPORT based on the data of the dashboard with the corresponding TLP AMBER designation.
HOW TO USE THIS DASHBOARD	Presents this document.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500