

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

V053023

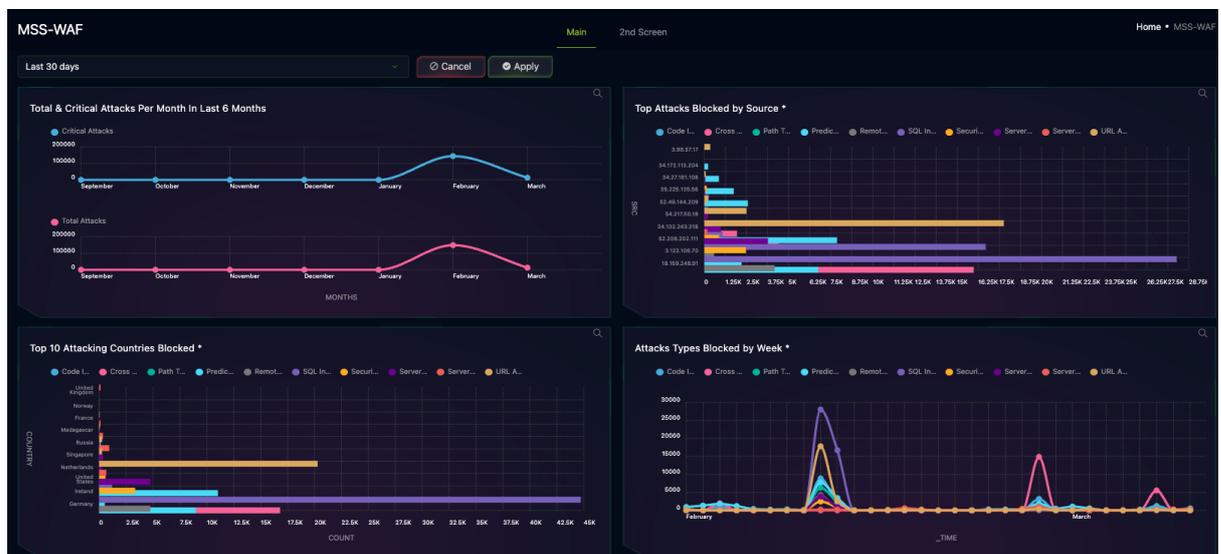
Revision V053023

*This document is a briefing that describes the operation and use of the Managed Web Application 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** 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





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

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

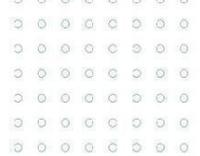
ITEM	DESCRIPTION
<b>Overview</b>	Displays the # of events blocked by the WAF.
<b>Blocked Events</b>	<p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours.</p> <p><b><i>This information can be used to quickly determine the number of attacks that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





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





	<b><i>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.</i></b>
<b>ON-DEMAND REPORT</b>	This action button will generate the MSS-WAF REPORT based on the data of the dashboard with the corresponding TLP AMBER designation.
<b>HOW TO USE THIS DASHBOARD</b>	Presents this document.

