



# MANAGED BREACH AND ATTACK SIMULATION

## Email VECTOR (MSS-BAS-Email)

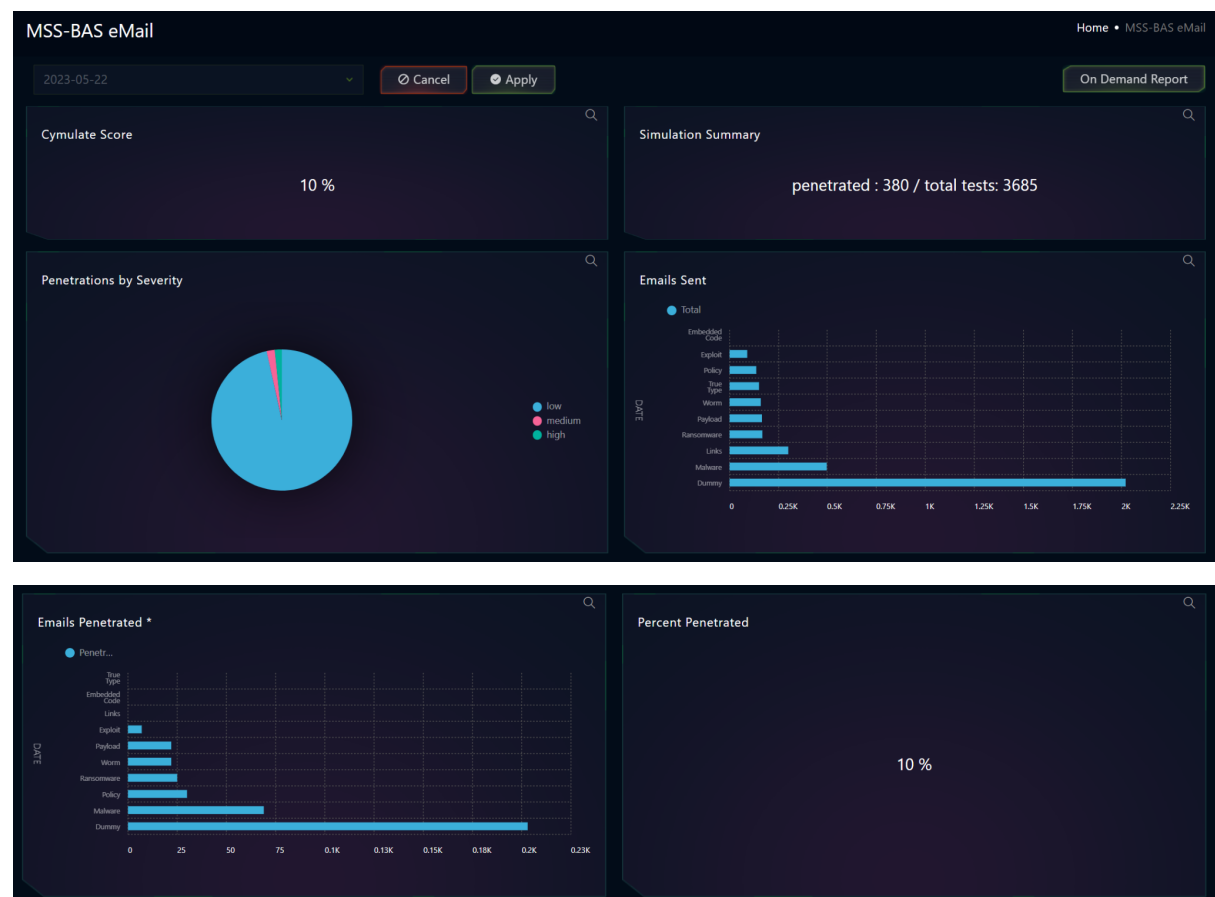
Revision V053023

*This document is a briefing that describes the operation and use of the Managed Bridge and Attack Simulation platform, 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-BAS** Service and the ability to generate an on-demand **report** for this service (with the information of the dashboard). These are 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 purposes.

The following presents the SKYWATCH MSS-BAS-Email





Simulations Sent/Penetrated			
	Category	Penetrated	Total
1	Dummy	205	2021
2	Malware	69	498
3	Links	0	299
4	Ransomware	25	167
5	Payload	22	165
6	Worm	22	159
7	True Type	0	150
8	Policy	30	136
9	Exploit	7	90
10	Embedded Code	0	0

## Detailed Description of functionality of the MSS-BAS-Email Dashboard

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

ITEM	DESCRIPTION
<b>Assessment Date Selector</b>	<p>Used to select which assessment's data is used to populate the dashboard's info modules. SKYWATCH stores assessment data for up to 30 days</p> <p><b>Automatically defaults to the last available assessment.</b></p>
<b>Cymulate Score</b>	<p>Displays the overall Cymulate score for all Email Vector Assessment. This module is not affected by the Assessment Date Selector.</p> <p>For SKYWATCH WEB the refresh rate is once a day.</p> <p><b><i>This information is used to determine overall performance of the Email vector.</i></b></p>
<b>Simulation Summary</b>	<p>Displays the number of attacks attempted during this assessment and how many successfully penetrated.</p> <p>For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector.</p> <p><b><i>This information is used to determine overall performance of the Email vector.</i></b></p>
<b>Penetrations by Severity</b>	<p>Displays the distribution of attack severities used during the assessment</p> <p>For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector.</p> <p><b><i>This information is used to determine how at risk a client is for high, medium, or low severity attacks.</i></b></p>
<b>Emails Sent</b>	<p>Displays the number and types of email attacks sent during the assessment</p> <p>For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector.</p> <p><b><i>This information is used to view the attack type distribution of the assessment.</i></b></p>
<b>Emails Penetrated</b>	<p>Displays the number of and types of email attacks that successfully penetrated the email inbox.</p>





	<p>For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector.</p> <p><i><b>This information is used to determine which email attack vector the client is particularly vulnerable to.</b></i></p>
<b>Percent Penetrated</b>	<p>Displays the percent of email attacks that successfully penetrated the email inbox.</p> <p>For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector.</p> <p><i><b>This information is used to determine overall performance of the Email vector</b></i></p>
<b>Simulations Sent/Penetrated</b>	<p>Displays the number of and types of email attacks sent in total</p> <p>For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector.</p> <p><i><b>This information is used to determine which email attack vector the client is particularly vulnerable to.</b></i></p>
<b>ON-DEMAND REPORT</b>	<p>This action button will generate the MSS-WAF REPORT based on the data of the dashboard with the corresponding TLP AMBER designation.</p>
<b>HOW TO USER THIS DASHBOARD</b>	<p>Presents this document.</p>

