



# MANAGED BREACH AND ATTACK SIMULATION DLP VECTOR (MSS-BAS-DLP)

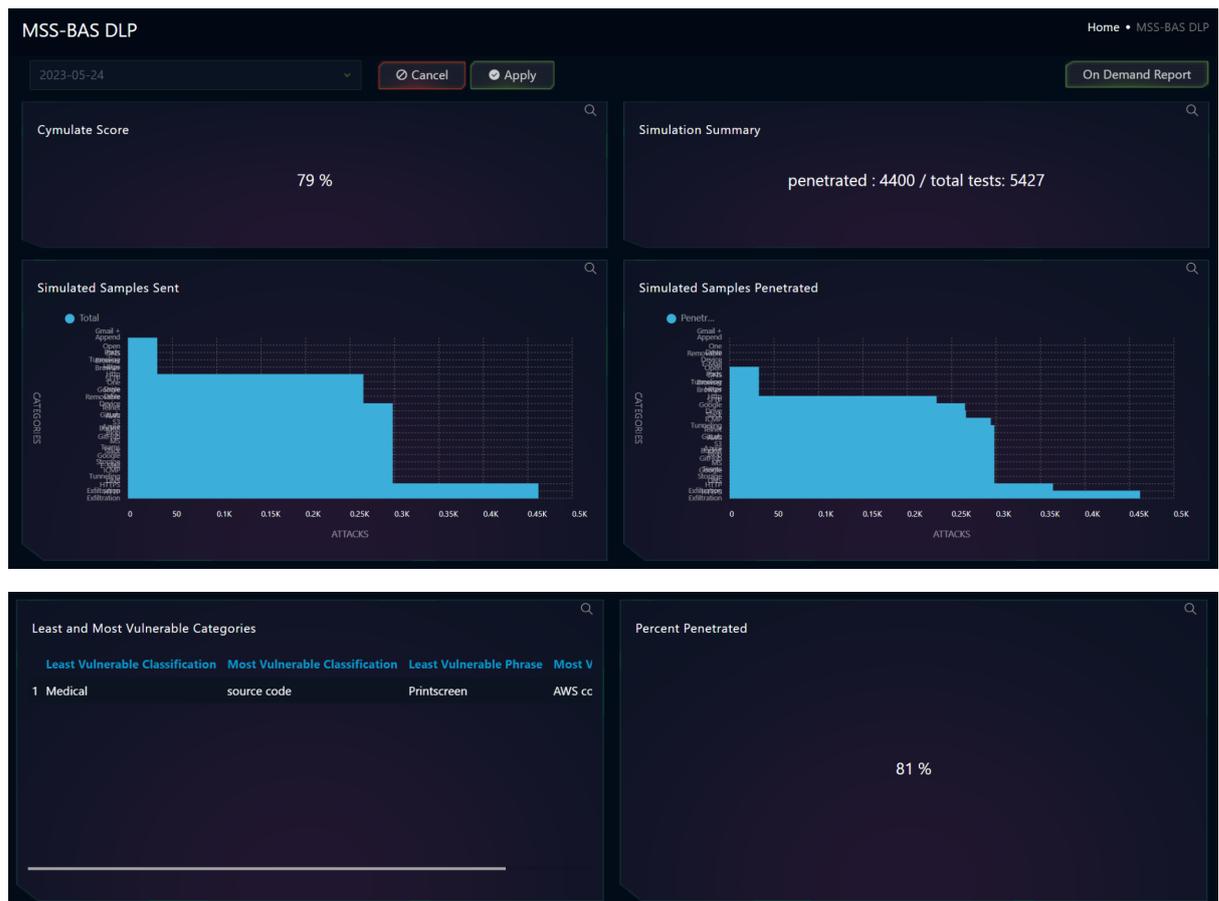
Revision V053023

*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-DLP





Simulations Sent/Penetrated			
	Category	Penetrated	Total
1	HTTP Exfiltration	364	462
2	HTTPS Exfiltration	462	462
3	DNS	298	298
4	ICMP Tunneling	294	298
5	E-Mail	0	298
6	Google Storage	298	298
7	Slack	266	298
8	MS Teams	298	298
9	GitHub	298	298
10	Azure Blob	298	298
11	AWS S3 Bucket	298	298
12	GitLab	298	298
13	Telnet	298	298
14	Removable Device	0	265
15	Google Drive	265	265
16	One Drive	0	265
17	SFTP	233	265

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

ITEM	DESCRIPTION
<b>Assessment Date Selector</b>	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  <b>Automatically defaults to the last available assessment.</b>
<b>Cymulate Score</b>	Displays the overall Cymulate score for all DLP Vector Assessment. This module is not affected by the Assessment Date Selector.  For SKYWATCH WEB the refresh rate is once a day.  <b><i>This information is used to determine overall performance of the DLP vector.</i></b>
<b>Simulation Summary</b>	Displays the number of attacks attempted during this assessment and how many successfully penetrated.  For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector.  <b><i>This information is used to determine overall performance of the DLP vector.</i></b>
<b>Least and Most Vulnerable Categories</b>	Displays the most and least vulnerable keywords and data types found to be susceptible to data leakage during the assessment.  For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector.  <b><i>This information is used to determine the most resistant and vulnerable data sources to data leakage.</i></b>
<b>Simulated Samples Sent</b>	Displays the number and types of data samples sent during the assessment.  For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector.





	<b><i>This information is used to view the attack type distribution of the assessment.</i></b>
<b>Simulated Samples Penetrated</b>	<p>Displays the number of and types of data samples that 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 which DLP attack vector the client is particularly vulnerable to.</i></b></p>
<b>Percent Penetrated</b>	<p>Displays the percent of data samples that 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 DLP vector</i></b></p>
<b>Simulations Sent/Penetrated</b>	<p>Displays the number of and types of DLP 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><b><i>This information is used to determine which DLP attack vector the client is particularly vulnerable to.</i></b></p>
<b>ON-DEMAND REPORT</b>	This action button will generate the MSS-BAS-DLP REPORT based on the data of the dashboard with the corresponding TLP AMBER designation.
<b>HOW TO USER THIS DASHBOARD</b>	Presents this document.

