GLESEC
COMPLETELY PERSPECTIVE

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

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.

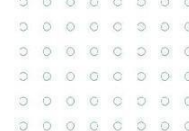The following presents the SKYWATCH MSS-BAS-EDR
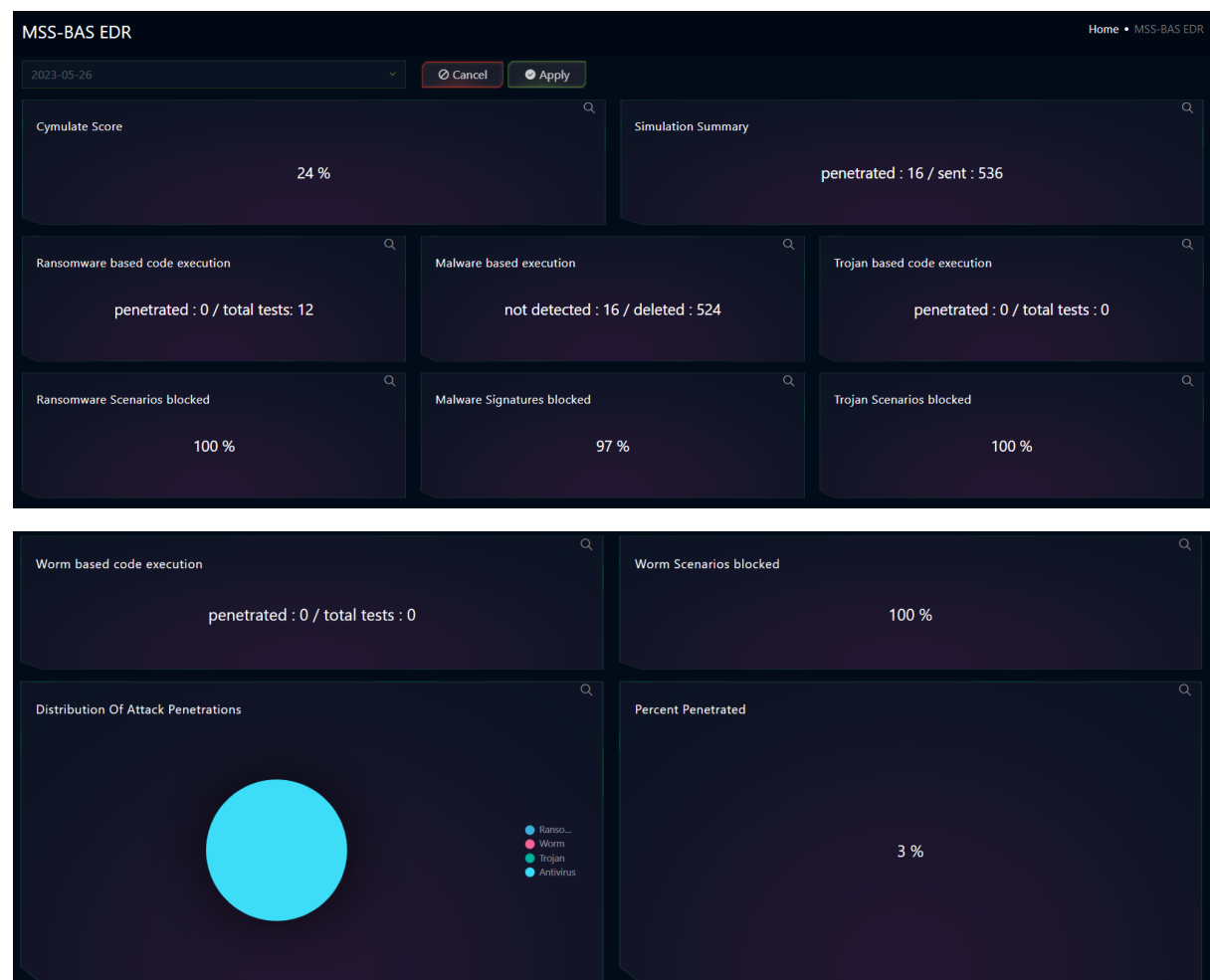
Simulations Sent/Penetrated

	Category	Penetrated	Total
1	Antivirus	16	524
2	Ransomware	0	12
3	Worm	0	0
4	Trojan	0	0

Detailed Description of functionality of the MSS-BAS-EDR Dashboard

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

ITEM	DESCRIPTION
Assessment Date Selector	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 **Automatically defaults to the last available assessment**.
Cymulate Score	Displays the overall Cymulate score for all EDR Vector Assessment. This module is not affected by the Assessment Date Selector. For SKYWATCH WEB the refresh rate is once a day. *This information is used to determine overall performance of the EDR vector.*
Simulation Summary	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. *This information is used to determine overall performance of the EDR vector.*
Ransomware based code execution.	Displays the number of ransomware 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. *This information is used to determine overall performance of the client's EDR solution against ransomware.*
Ransomware Scenarios blocked	Displays the percentage of ransomware attacks blocked during this assessment. For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector. *This information is used to determine overall performance of the client's EDT solution against ransomware.*
Malware based execution	Displays the number of malware 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.

GLESEC

LATAM HQ
+507   836-5355

US HQ
+1 (321) 430-0500

PROPRIETARY & CONFIDENTIAL

	This information is used to determine overall performance of the client's EDR solution against malware.
Malware Signatures Blocked	Displays the percentage of malware attacks blocked during this assessment. For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector. *This information is used to determine overall performance of the client's EDR solution against malware.*
Trojan based code execution	Displays the number of trojan 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. *This information is used to determine overall performance of the client's EDR solution against trojans.*
Trojan Scenarios Blocked	Displays the percentage of trojan attacks blocked during this assessment. For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector. *This information is used to determine overall performance of the client's EDR solution against trojans.*
Worm based code execution.	Displays the number of worm 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. *This information is used to determine overall performance of the client's EDR solution against worms.*
Worm Scenarios Blocked	Displays the percentage of worm attacks blocked during this assessment. For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector. *This information is used to determine overall performance of the client's EDR solution against worms.*
Percent Penetrated	Displays the percent of EDR attacks that successfully penetrated. For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector. *This information is used to determine overall performance of the EDR vector*
Distribution of Attack Types Penetrated	Displays the distribution of attack types that penetrated used 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. *This information is used to determine how at risk a client is for a particular type of attack.*
Simulations Sent/Penetrated	Displays the number of and types of EDR attacks sent in total For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the date selector. *This information is used to determine which EDT attack vector the client is particularly vulnerable to.*

GLESEC

LATAM HQ
+507   836-5355

US HQ
+1 (321) 430-0500

PROPRIETARY & CONFIDENTIAL

ON-DEMAND REPORT	This action button will generate the MSS-BAS-EDR REPORT based on the data of the dashboard with the corresponding TLP AMBER designation.
HOW TO USER THIS DASHBOARD	Presents this document.