MANAGED BREACH AND ATTACK SIMULATIO
IMMEDIATE THREAT VECTOR (MSS-BAS-IMTHREAT)

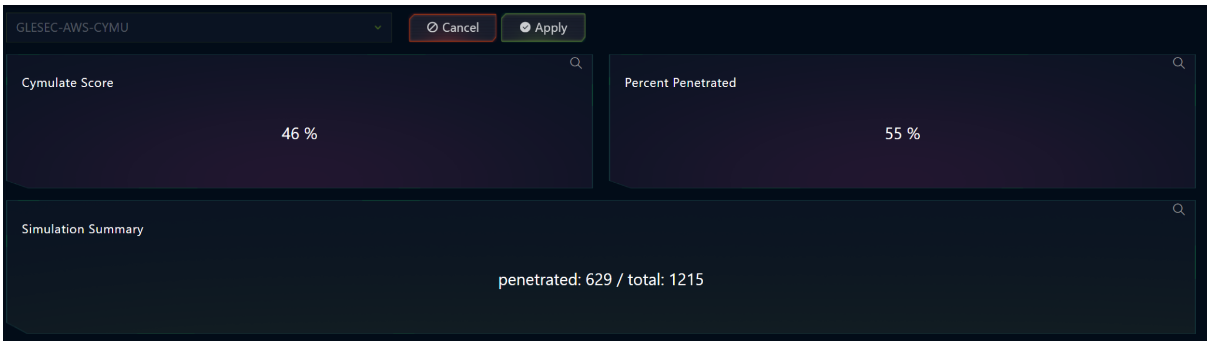
Revision V053023

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.

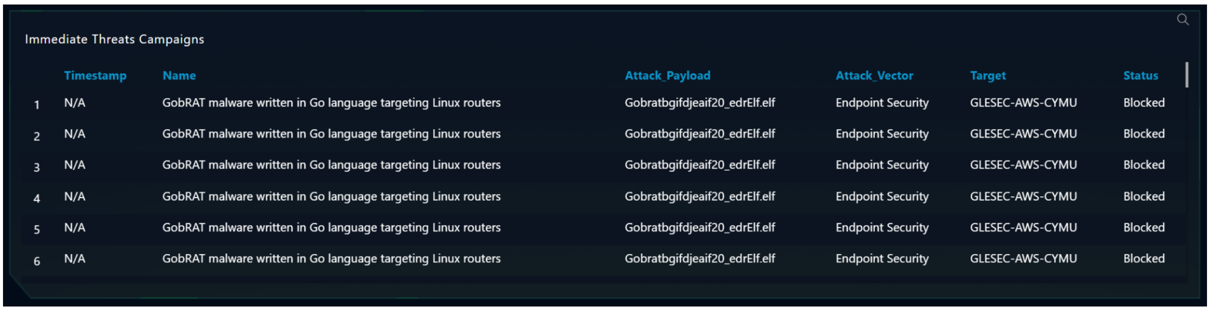
The following presents the SKYWATCH MSS-BAS-IMTHREAT



Cymulate Score: 46 %

Percent Penetrated: 55 %

Simulation Summary: penetrated: 629 / total: 1215



Immediate Threats Campaigns

	Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
1	N/A	GobRAT malware written in Go language targeting Linux routers	Gobratbgifdjeaif20_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2	N/A	GobRAT malware written in Go language targeting Linux routers	Gobratbgifdjeaif20_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
3	N/A	GobRAT malware written in Go language targeting Linux routers	Gobratbgifdjeaif20_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
4	N/A	GobRAT malware written in Go language targeting Linux routers	Gobratbgifdjeaif20_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
5	N/A	GobRAT malware written in Go language targeting Linux routers	Gobratbgifdjeaif20_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
6	N/A	GobRAT malware written in Go language targeting Linux routers	Gobratbgifdjeaif20_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked

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

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

ITEM	DESCRIPTION
Agent **Target Selector**	Used to select which agent's data is used to populate the dashboard's info modules. SKYWATCH stores assessment data for up to 30 days.

Cymulate Score	Displays the overall Cymulate score for all IMTHREAT Vector Assessment. This module is not affected by the Agent Target Selector. For SKYWATCH WEB the refresh rate is once a day. ***This information is used to determine overall performance of the IMTHREAT 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 target selector. ***This information is used to determine overall performance of the IMTHREAT vector.***
Percent Penetrated	Displays the percent of immediate threat attacks that successfully penetrated. For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the target selector. ***This information is used to determine overall performance of the IMTHREAT vector.***
Immediate Threat campaigns	Displays a list of the most recent immediate threat campaigns tested on the selected agent machine. For SKYWATCH WEB the refresh rate is once a day. The information represents data from the assessment selected in the target selector. ***This information is used to determine what immediate threats the target agent is vulnerable to.***
ON-DEMAND REPORT	This action button will generate the MSS-BAS-IMTHREAT REPORT based on the data of the dashboard with the corresponding TLP AMBER designation.
HOW TO USER THIS DASHBOARD	Presents this document.