GLESEC
COMPLETELY PERSPECTIVE

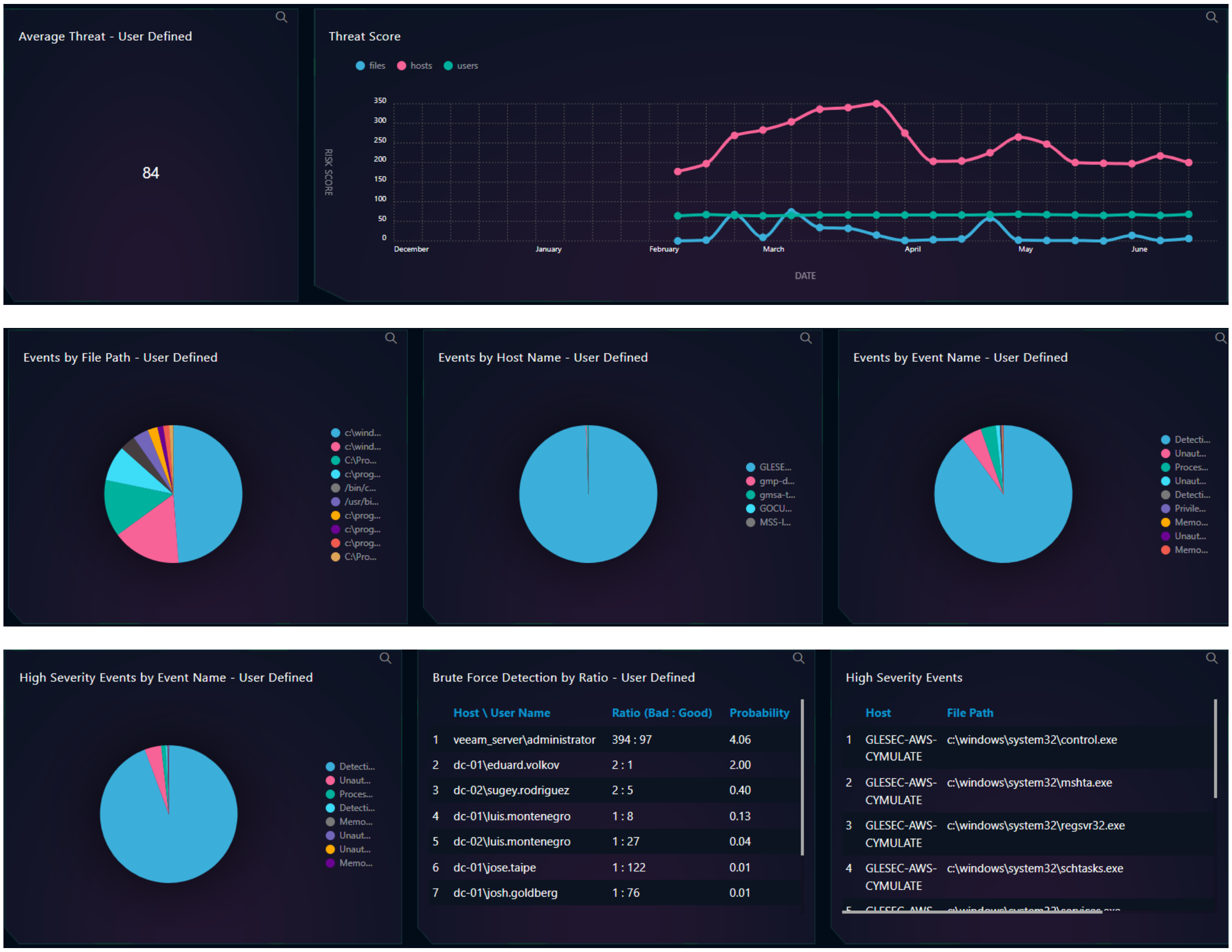
ENDPOINT DETECTION AND RESPONSE SERVICE (MSS-EDR)

This document is a briefing that describes the operation and use of the Endpoint Detection and Response Service, and it is meant for all users of SKYWATCH WEB Platform.

Purpose of this Dashboard

This SKYWATCH Dashboard(s) provides **visibility** to the technical and executive users of SKYWATCH about the **MSS-EDR** Service and an on-demand **report** for this service (with the information of the dashboard). These are two of the deliverables for this 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) into action to further investigate and for incident-response.

The following presents the SKYWATCH MSS-EDR.

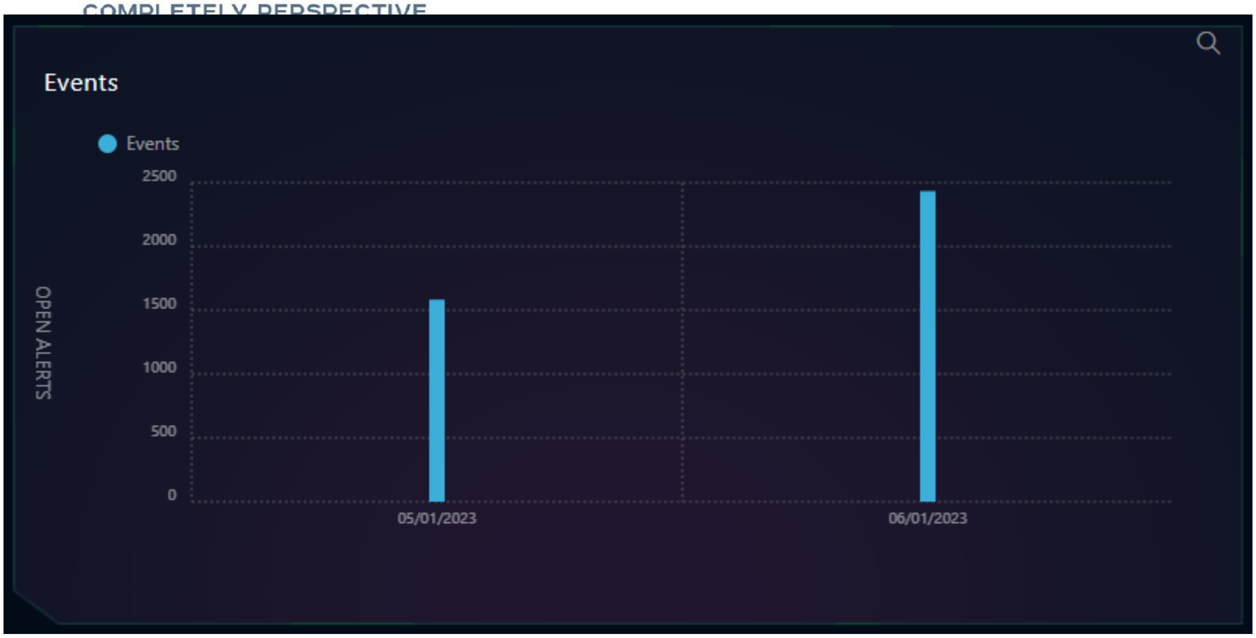


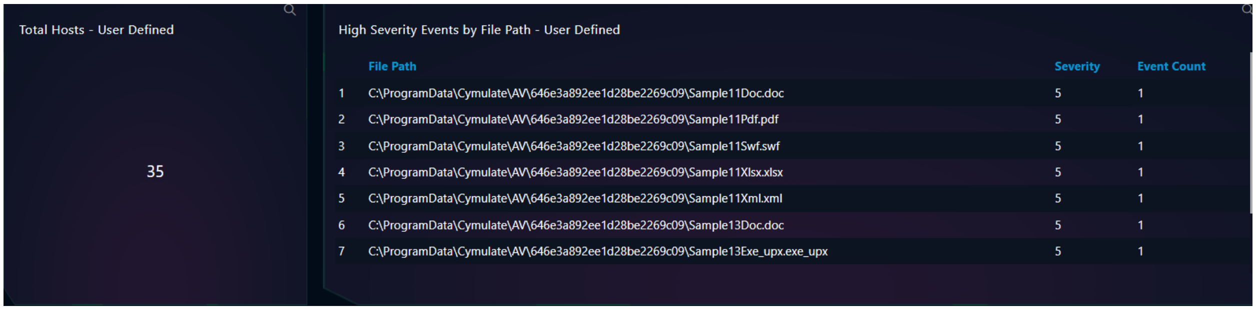
Brute Force Detection by Ratio - User Defined

	Host \ User Name	Ratio (Bad : Good)	Probability
1	veeam_server\administrator	394 : 97	4.06
2	dc-01\eduard.volkov	2 : 1	2.00
3	dc-02\sugey.rodriguez	2 : 5	0.40
4	dc-01\luis.montenegro	1 : 8	0.13
5	dc-02\luis.montenegro	1 : 27	0.04
6	dc-01\jose.taipe	1 : 122	0.01
7	dc-01\josh.goldberg	1 : 76	0.01

High Severity Events

	Host	File Path
1	GLESEC-AWS-CYMULATE	c:\windows\system32\control.exe
2	GLESEC-AWS-CYMULATE	c:\windows\system32\mshta.exe
3	GLESEC-AWS-CYMULATE	c:\windows\system32\regsvr32.exe
4	GLESEC-AWS-CYMULATE	c:\windows\system32\schtasks.exe
5	GLESEC-AWS-	c:\windows\system32\services.exe





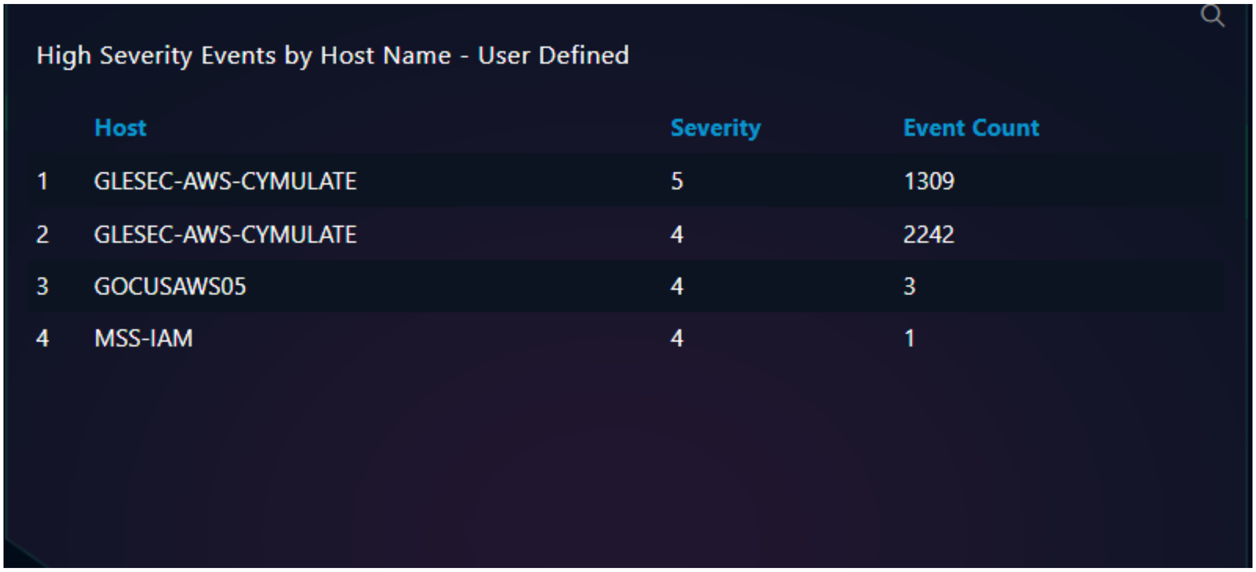
Total Hosts - User Defined

35

High Severity Events by File Path - User Defined

	File Path	Severity	Event Count
1	C:\ProgramData\Cymulate\AV\646e3a892ee1d28be2269c09\Sample11Doc.doc	5	1
2	C:\ProgramData\Cymulate\AV\646e3a892ee1d28be2269c09\Sample11Pdf.pdf	5	1
3	C:\ProgramData\Cymulate\AV\646e3a892ee1d28be2269c09\Sample11Swf.swf	5	1
4	C:\ProgramData\Cymulate\AV\646e3a892ee1d28be2269c09\Sample11Xlsx.xlsx	5	1
5	C:\ProgramData\Cymulate\AV\646e3a892ee1d28be2269c09\Sample11Xml.xml	5	1
6	C:\ProgramData\Cymulate\AV\646e3a892ee1d28be2269c09\Sample13Doc.doc	5	1
7	C:\ProgramData\Cymulate\AV\646e3a892ee1d28be2269c09\Sample13Exe_upx.exe_upx	5	1

su



High Severity Events by Host Name - User Defined

	Host	Severity	Event Count
1	GLESEC-AWS-CYMULATE	5	1309
2	GLESEC-AWS-CYMULATE	4	2242
3	GOCUSAWS05	4	3
4	MSS-IAM	4	1

Detailed Description of functionality of the MSS-EDR Dashboard

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

ITEM	DESCRIPTION
Average Threat - User Defined	Displays the average threat score for users over a certain time span. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to monitor if the average threat for users has been recently increasing or decreasing.
Threat Score	Displays the threat score for files hosts and users over a 6-month span. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 6 months. This information can be used to monitor these three fields and compare them to each other as well as see any differences in each month.
Events by File Path - User Defined	Displays recent events that occurred in the files for a user. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to see what file additions could be potentially dangerous to the users and where it can be found.
Events by Host Name - User Defined	Displays recent events that occurred on a host machine. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to see your top 5 machines that have had events called and which ones are getting the most traffic.
Events by Event Name - User Defined	Displays the top recent events that have occurred between all of your machines for a user. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to see which event is the most popular and should be worked on or looked at.
High Severity Events by Event Name - User Defined	Displays the top recent high events that have occurred between all of your machines for a user. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to see which high event is the most popular and should be worked on or looked at.
Brute Force Detection by Ratio - User Defined	Displays a ratio of successful logins and unsuccessful logins for a user. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to see which users have an unexpected high number of bad logins and should be monitored.

High Severity Events	Displays a list of high severity events, showing the machine that it belongs to as well as the file path that it is found in. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 24 hours. This information can be used to see which specific high severity event is affecting what computer and where the possible problem lies.
Events	Displays the total amount of events that have occurred in the current and previous month. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 6 months. This information can be used to see if your total events between the two months have gone up or down.
Total Hosts - User Defined	Displays the total machines connected to the EDR. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to see how many active machines you have being monitored by the EDR.
High Severity Events by File Path - User Defined	Displays recent high severity events that occurred in the files for a user. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to see what file additions could be potentially dangerous to the users and where it can be found.
High Severity Events by Host Name - User Defined	Displays recent high severity events that occurred on a host machine. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to see your top machines that have had events called and which ones are getting the most traffic.
REPORT	This action button will generate a MSS-EDR REPORT based on the data of the dashboard with the corresponding TLP AMBER designation.