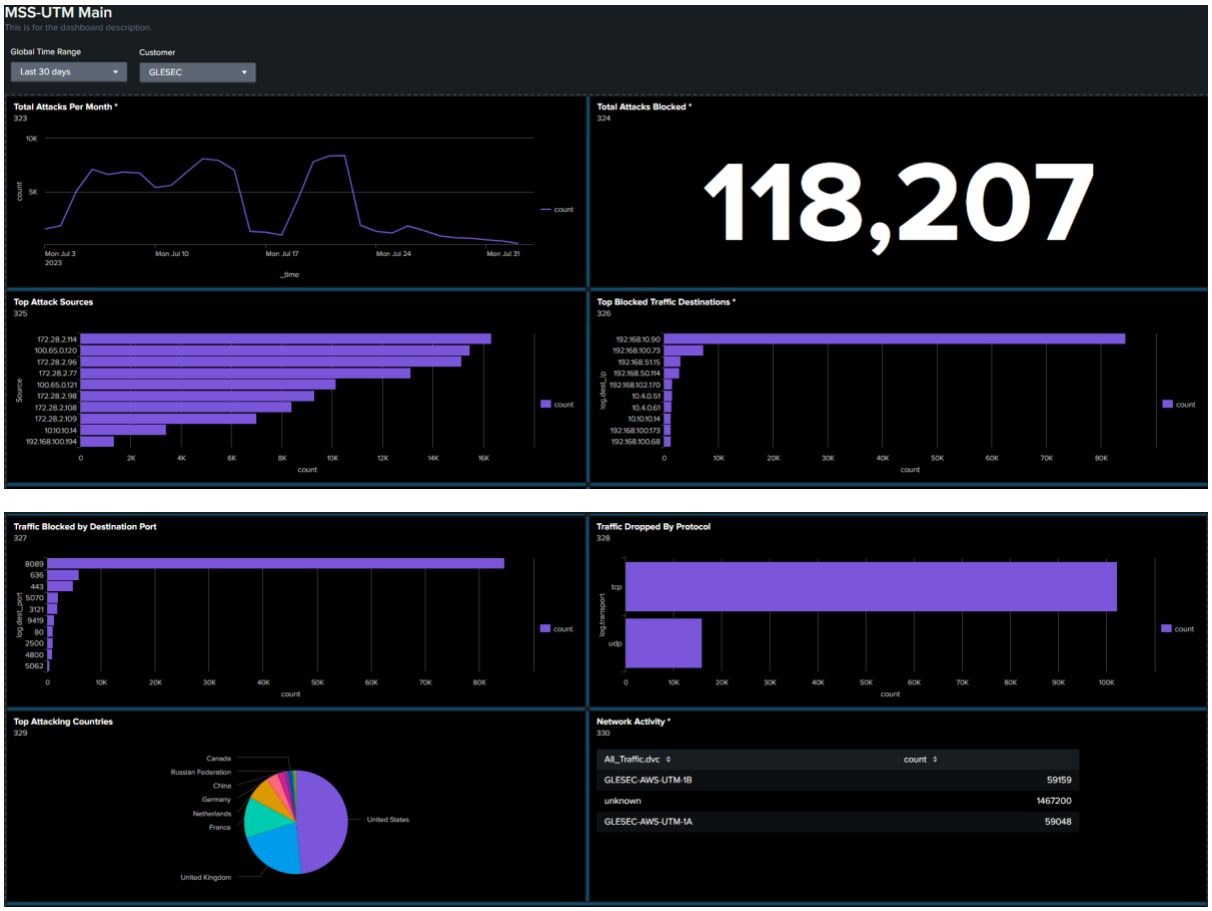
MANAGED UNIFIED THREAT MANAGEMENT SERVICE (MSS-UTM)

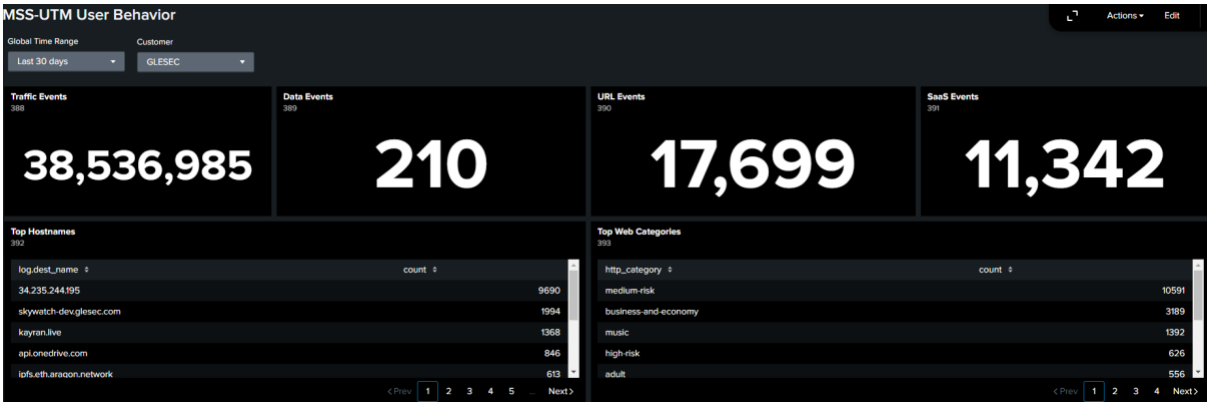
This document is a briefing that describes the operation and use of the Managed Unified Threat Management, and it is meant for all users of SKYWATCH WEB Platform.

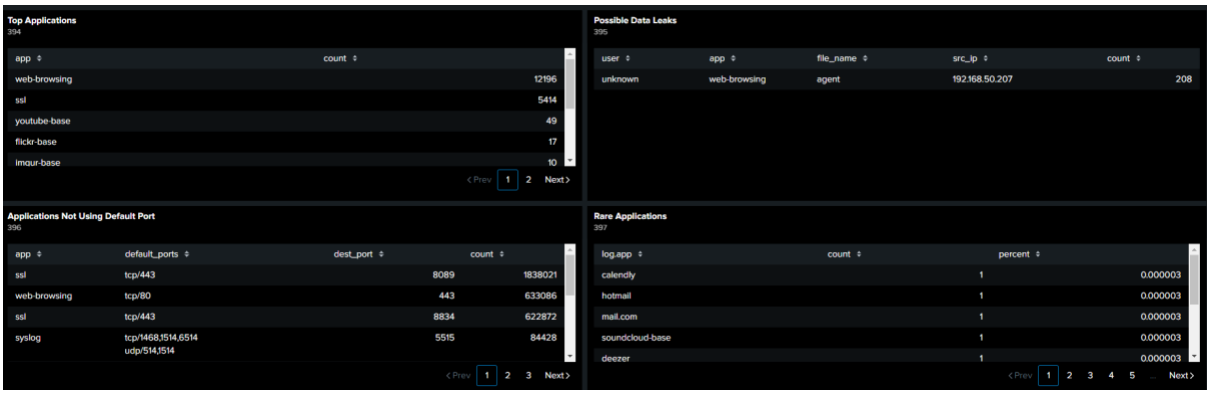
Purpose of this Dashboard

This SKYWATCH Dashboard(s) provide **visibility** to the technical and executive users of SKYWATCH for the **MSS-UTM** Service and the ability to generate an on-demand **report** for this service (with the information of the dashboard). These are two of 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 action to further investigate and for incident-response purpose.

The following presents the SKYWATCH MSS-UTM.

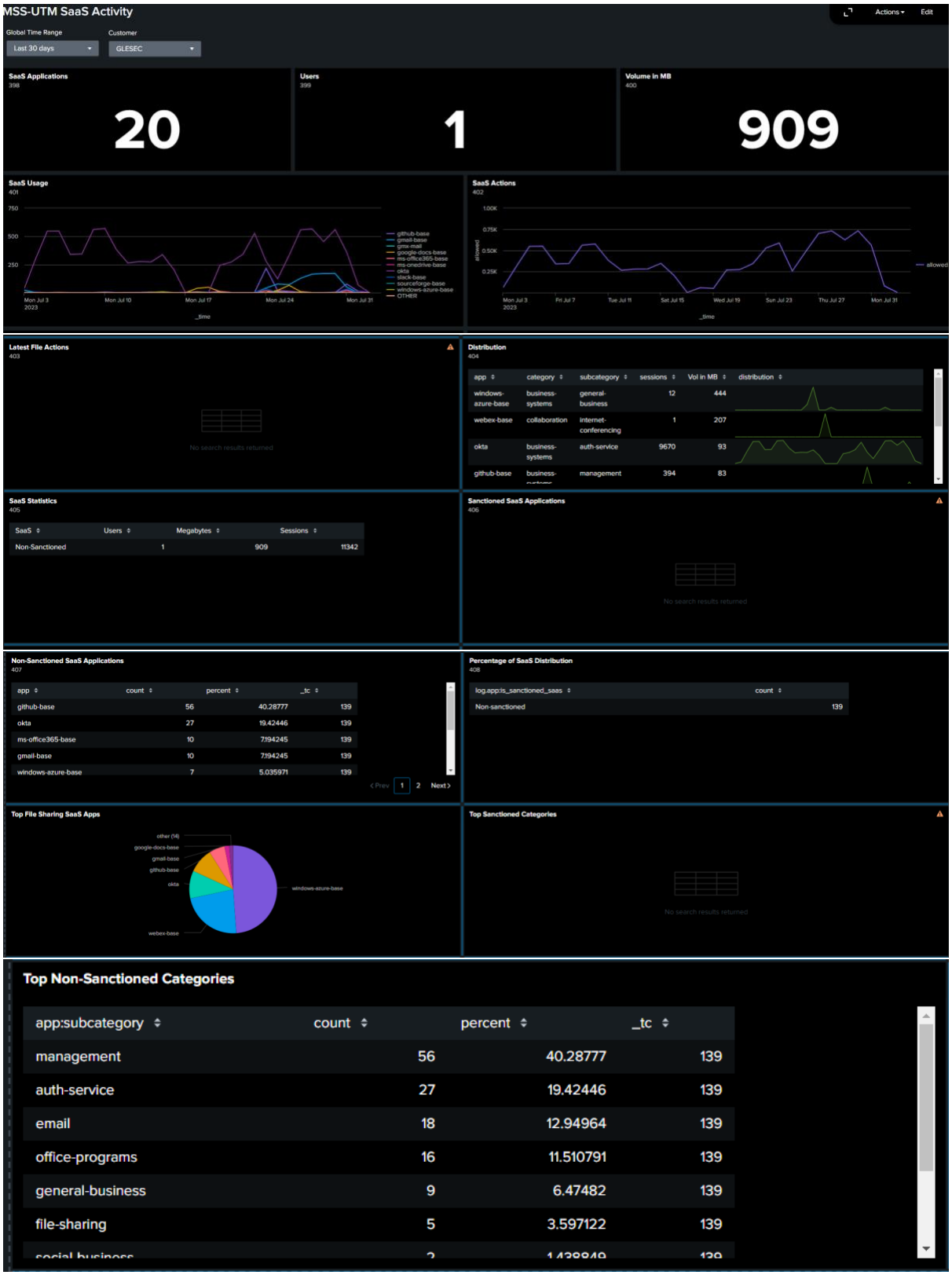


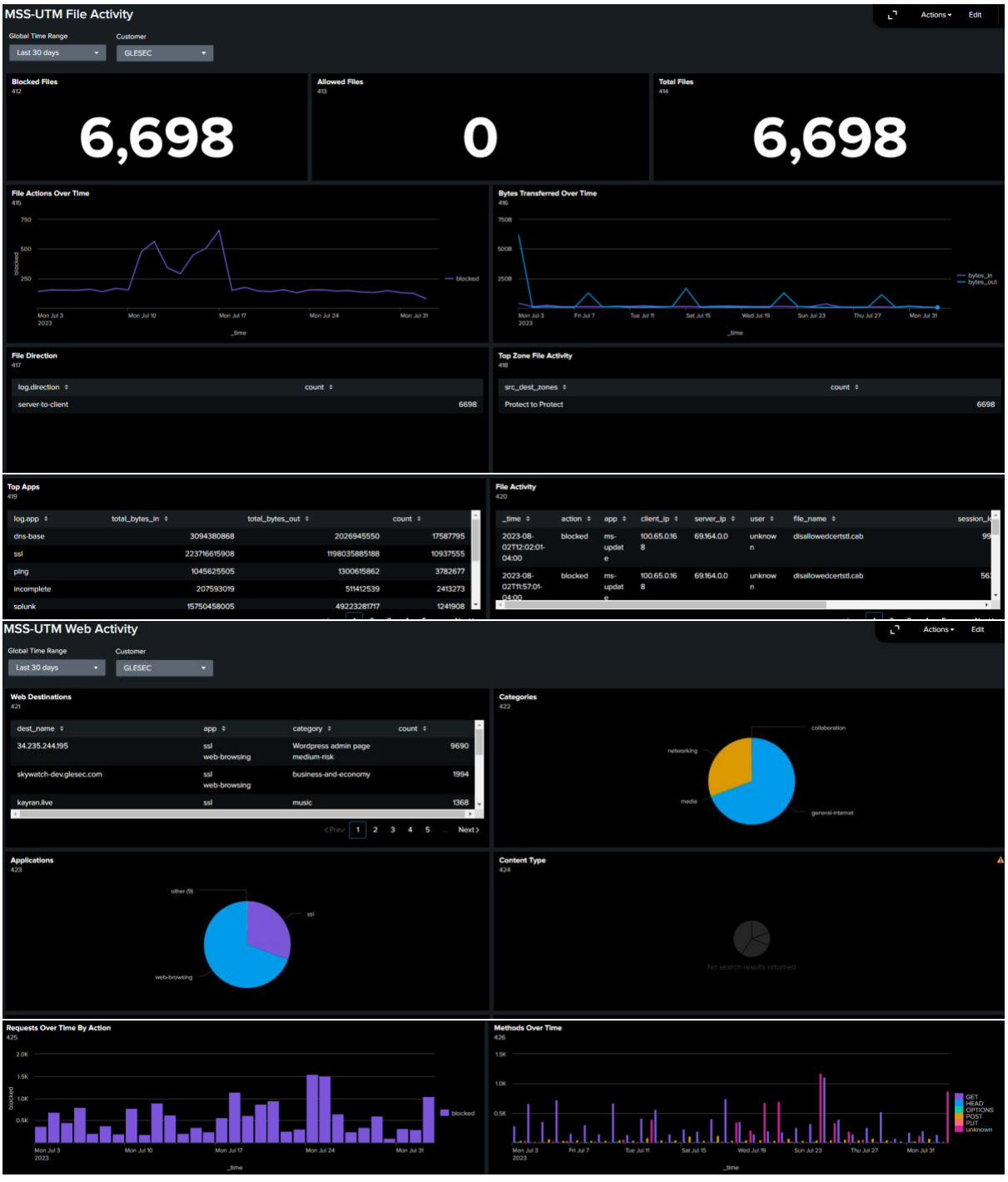


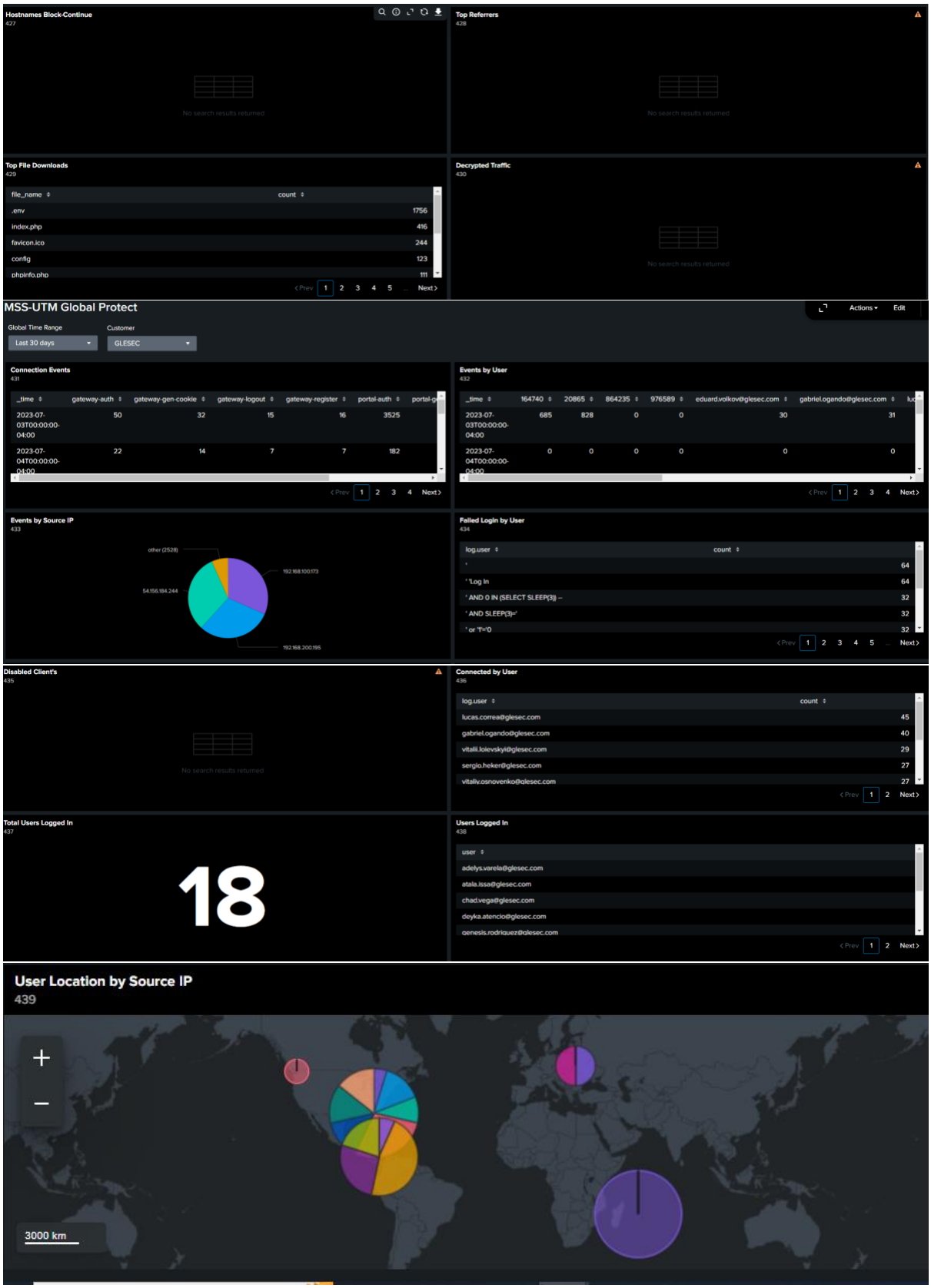


LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500


MSS-UTM SaaS Activity
Actions
Edit
Global Time Range
Last 30 days
Customer
GLESEC
SaaS Applications
398
20
Users
399
1
Volume in MB
400
909
SaaS Usage
401
SaaS Actions
402
Latest File Actions
403
No search results returned
Distribution
404
app
category
subcategory
sessions
Vol in MB
distribution
windows-azure-base
business-systems
general-business
12
444
webex-base
collaboration
internet-conferencing
1
207
okta
business-systems
auth-service
9670
93
github-base
management
394
83
SaaS Statistics
405
SaaS
Users
Megabytes
Sessions
Non-Sanctioned
1
909
11342
Sanctioned SaaS Applications
406
No search results returned
Non-Sanctioned SaaS Applications
407
app
count
percent
_tc
github-base
56
40.28777
139
okta
27
19.42446
139
ms-office365-base
10
7.194245
139
gmail-base
10
7.194245
139
windows-azure-base
7
5.035971
139
Percentage of SaaS Distribution
408
log.app:is_sanctioned_saas
count
Non-sanctioned
139
Top File Sharing SaaS Apps
Top Sanctioned Categories
No search results returned
Top Non-Sanctioned Categories
app:subcategory
count
percent
_tc
management
56
40.28777
139
auth-service
27
19.42446
139
email
18
12.94964
139
office-programs
16
11.510791
139
general-business
9
6.47482
139
file-sharing
5
3.597122
139


MSS-UTM File Activity
Actions
Edit
Global Time Range
Last 30 days
Customer
GLESEC
Blocked Files
412
6,698
Allowed Files
413
0
Total Files
414
6,698
File Actions Over Time
415
blocked
Bytes Transferred Over Time
416
bytes_in
bytes_out
File Direction
417
log.direction
count
server-to-client
6698
Top Zone File Activity
418
src_dest_zones
count
Protect to Protect
6698
Top Apps
419
log.app
total_bytes_in
total_bytes_out
count
dns-base 3094380868 2026945550 17587795
ssl 223716615908 1198035885188 10937555
ping 1045625505 1300615862 3782677
incomplete 207593019 511412539 2413273
splunk 15750458005 49223281717 1241908
File Activity
420
_time
action
app
client_ip
server_ip
user
file_name
2023-08-02T12:02:01-04:00 blocked ms-update 100.65.0.16 69.164.0.0 unknown disallowedcertstl.cab
2023-08-02T11:57:01-04:00 blocked ms-update 100.65.0.16 69.164.0.0 unknown disallowedcertstl.cab
MSS-UTM Web Activity
Actions
Edit
Global Time Range
Last 30 days
Customer
GLESEC
Web Destinations
421
dest_name
app
category
count
34.235.244.195 ssl web-browsing Wordpress admin page medium-risk 9690
skywatch-dev.glesec.com ssl web-browsing business-and-economy 1994
kayran.live ssl music 1368
Prev 1 2 3 4 5 Next
Categories
422
collaboration
networking
media
general-internet
Applications
423
other (9)
ssl
web-browsing
Content Type
424
No search results returned
Requests Over Time By Action
425
blocked
Methods Over Time
426
GET
HEAD
OPTIONS
POST
PUT
unknown


Hostnames Block-Continue
427
No search results returned
Top Referrers
428
No search results returned
Top File Downloads
429
file_name
count
.env
1756
index.php
416
favicon.ico
244
config
123
phpinfo.php
111
Prev 1 2 3 4 5 Next
Decrypted Traffic
430
No search results returned
MSS-UTM Global Protect
Actions
Edit
Global Time Range
Last 30 days
Customer
GLESEC
Connection Events
431
_time
gateway-auth
gateway-gen-cookie
gateway-logout
gateway-register
portal-auth
2023-07-03T00:00:00-04:00
50
32
15
16
3525
2023-07-04T00:00:00-04:00
22
14
7
7
182
Prev 1 2 3 4 Next
Events by User
432
_time
164740
20865
864235
976589
eduard.volkov@glesec.com
gabriel.ogando@glesec.com
2023-07-03T00:00:00-04:00
685
828
0
0
30
31
2023-07-04T00:00:00-04:00
0
0
0
0
0
0
Prev 1 2 3 4 Next
Events by Source IP
433
other (2528)
192.168.100.173
54.156.184.244
192.168.200.195
Failed Login by User
434
log.user
count
'
64
' 'Log In
64
' AND 0 IN (SELECT SLEEP(3)) --
32
' AND SLEEP(3)='
32
' or '1'='0
32
Prev 1 2 3 4 5 Next
Disabled Client's
435
No search results returned
Connected by User
436
log.user
count
lucas.correa@glesec.com
45
gabriel.ogando@glesec.com
40
vitalii.loievskyi@glesec.com
29
sergio.heker@glesec.com
27
vitaliy.osnovenko@glesec.com
27
Prev 1 2 Next
Total Users Logged In
437
18
Users Logged In
438
user
adelys.varela@glesec.com
atala.issa@glesec.com
chad.vega@glesec.com
deyka.atencio@glesec.com
genesis.rodriguez@glesec.com
Prev 1 2 Next
User Location by Source IP
439
3000 km

Detailed Description of functionality of the MSS-UTM Dashboard

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

ITEM	DESCRIPTION
Main	
Total Attacks Per Month	Displays the # of hits made by bots. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used as an indicator of the amount of detected bot activity.
Total Attacks Blocked	Displays the total # of hits that were blocked all time. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to keep track of how many bot attacks have been blocked in total.
Top Attack Sources	Displays the top 10 attack source ips. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see what ips are sending the most attacks and should be monitored more.
Top Blocked Traffic Destinations	Displays the top 10 traffic destinations that have been blocked. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see what ips are being blocked the most and if this is expected.
Traffic Blocked by Destination Port	Displays the top 10 destination ports that have traffic blocked. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see what ports are having traffic blocked and if this is expected.
Traffic Dropped by Protocol	Displays the amount of traffic that is dropped per protocol. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see which of your protocols has more traffic that is being blocked and if this is expected.
Top Attacking Countries	Displays in a pie chart what are the top attacking countries. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see which countries are sending the most bot attacks.
Network Activity	Displays in a table which network all of the traffic is occurring on. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

	This information can be used to see what network most of your traffic is happening on and if this is expected.
Traffic Blocked by Rule	Displays in a table the amount of traffic that is blocked by firewall rules. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see which of your rules is blocking the most and least amount of traffic.
Blocked Traffic & Security Alert Destination IP Address	Displays in a heat map where traffic and security alerts are being created by destination ips. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see which countries' destination ips are receiving the most blocked traffic and security alerts.
Blocked Traffic & Security Alert Source IP Address	Displays in a heat map where traffic and security alerts are being created by source ips. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see which countries' source ips are receiving the most blocked traffic and security alerts.
User Behavior	
Traffic Events	Displays the number of bot signatures detected over the last 24 hours. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to indicate the number of unique bots that were detected.
Data Events	Displays the number of data events detected over the last 24 hours. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to indicate the number of unique data events that were detected.
URL Events	Displays the number of URL events detected over the last 24 hours. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to indicate the number of unique URL events that were detected.
SaaS Events	Displays the number of SaaS events detected over the last 24 hours. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to indicate the number of unique SaaS events that were detected.
Top Hostnames	Displays a table of the top hostname destinations that URL events are occuring. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see which hosts have the most events appearing at.

Top Web Categories	Displays a table of the top web categories that URL events are occuring. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see which web categories have the most events appearing at.
Top Applications	Displays a table of the top applications that URL events are occuring. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see which applications are being used the most.
Possible Data Leaks	Displays a table of possible data leaks, where they occurred and what could be causing it. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to verify if there is a possible data leak on a machine or application.
Applications Not Using Default Port	Displays a table of applications that are not using the default ports. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to check what applications are currently not using the default ports and if that is correct.
Rare Applications	Displays a table of applications that are rarely used. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to check if there is an application that no one should be using but is being used every now and then.
SaaS Activity	
SaaS Applications	Displays the number of unique transactions made by bots. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to indicate the number of unique transactions made by bots.
Users	Displays the number of users that have SaaS activity. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to track how many users are using SaaS.
Volume in MB	Displays the number of volumes in MB being used in SaaS activities. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to show how much volume is being used in SaaS.
SaaS Usage	Displays a line chart of what is using SaaS in the last month. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month.

	This information can be used to see which SaaS applications are being used the most and when they are being used.
SaaS Actions	Displays a line chart over the last month of allowed SaaS actions. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month. This information can be used to see how many SaaS actions were allowed throughout the month.
Latest File Actions	Displays a table of the latest file actions that have occurred in SaaS. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see what file actions have recently taken place.
Distribution	Displays a table of the distribution of the SaaS applications. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see what applications are being used the most, and how often they are being used.
SaaS Statistics	Displays a table of sanctioned and non-sanctioned SaaS applications. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see if SaaS applications are approved or not before use.
Sanctioned SaaS Applications	Displays a table of sanctioned SaaS applications. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see which sanctioned SaaS applications are being used the most and least.
Non-Sanctioned SaaS Applications	Displays a table of non-sanctioned SaaS applications. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see which non-sanctioned SaaS applications are being used the most and least.
Percentage of SaaS Distribution	Displays a table that shows the percentage of non-sanctioned and sanctioned SaaS applications. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see a numerical value of the usage of non-sanctioned applications versus sanctioned applications.
Top FIle Sharing SaaS Apps	Displays a pie chart with SaaS apps that have file sharing. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to see which file sharing SaaS apps are being used the most or least.
Top Sanctioned Categories	Displays a table of the top sanctioned categories.

	For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to monitor which sanctioned categories are being used the most and least.
Top Non-Sanctioned Categories	Displays a table of the top non-sanctioned categories. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to monitor which non-sanctioned categories are being used the most and least.
File Activity	
Blocked FIles	Displays the number of unique paths accessed by bots. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month. This information can be used to get an idea of how many unique resources that were accessed by bots.
Allowed Files	Displays the number of allowed files. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month. This information can be used to see how many files are being allowed through the file blocking.
Total Files	Displays the number of total files. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month. This information can be used to see if the number of allowed files and blocked files add up to the total files.
File Actions Over Time	Displays a line chart of what file actions occurred in the last month. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month. This information can be used to see a graphical view of when files were blocked or allowed in the last month.
Bytes Transferred Over Time	Displays a line chart of the bytes transferred over the last month. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month. This information can be used to monitor how many bytes were going in and out.
File Direction	Displays a table of the direction that files are going in the server. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month. This information can be used to see the direction your files are going.
Top Zone File Activity	Displays a table of the zone file activity. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month. This information can be used to see which zones your files are moving between.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Top Apps	Displays a table of the top applications that are being used with the files. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month. This information can be used to see which applications have the most and least byte activity.
File Activity	Displays a table of file activity. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month. This information can be used to see whether the files are being blocked or allowed, the name of the files, on what machines they were transferring between, and the zones they were moving between.
Web Activity	
Web Destinations	Displays a table that shows the web destinations occurring. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to show where the web destinations are taking place, what category they fall under, what app they are considered, and how often they are occurring.
Categories	Displays a pie chart that shows the categories of bots that have been detected. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to determine the most common category of bot threats.
Applications	Displays a pie chart that shows the applications of bots that have been detected. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to determine the most common application of bot threats.
Content Type	Displays a pie chart that shows the content of bots that have been detected. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to determine the most common content of bot threats.
Requests Over Time by Action	Displays a bar chart that shows how many requests were blocked in the last month. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month. This information can be used to show when the most or least web activity was blocked.
Methods over Time	Displays a bar chart of the different methods that were being used with web activity in the last month. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last month. This information can be used to show when the most or least methods were blocked
Hostnames Block-Continue	Displays a table of hostnames that were blocked or allowed. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours.

	This information can be used to show what hostnames are being blocked or allowed and can be used to verify if those are correct.
Top Referrers	Displays a table of the top referrers that occurred. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to show what referrers are occurring the most or least.
Top FIle Downloads	Displays a table of the top file downloads on the web. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to show which types of files are being downloaded the most and least.
Decrypted Traffic	Displays a table of traffic that was decrypted. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to show which traffic was able to be decrypted and should be looked at.
Global Protect	
Connection Events	DIsplays a horizontal bar chart showing IPs of the top 5 bots. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to determine where most bot attacks originate from.
Events by User	Displays a bar chart of how many events were done by a user on Global Protect and when it occurred. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to show which users are using Global Protect the most and when they were using it.
Events by Source IP	Displays a pie chart of how many events occurred by source ip. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to show what source ip has the most events occurring while connected to Global Protect.
Failed Login by User	Displays a table of users that failed to login. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to show what users are having trouble logging in the most and if any of them are potential threats.
Disabled Clients	Displays a table of clients that are disabled from logging into Global Protect. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to monitor clients that should not have access to Global Protect.
Connected by User	Displays a table of how many times a user connects to Global Protect.

	For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to monitor the usage of Global Protect by the user.
Total Users Logged In	Displays a number of the total current users logged into Global Protect. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to monitor how many users are currently connected to Global Protect.
Users Logged In	Displays a table of the users currently logged into Global Protect. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to monitor who is currently connected to Global Protect.
User Location by Source IP	Displays a pie chart on a map of the users location by source ip that are connected to Global Protect. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from the last 24 hours. This information can be used to monitor where your users are connecting to Global Protect from.