Grideye Central - Web API

Last updated by | Bala Palaniyappan | Jun 19, 2022 at 11:06 AM GMT+5:30

Use http://grideyedemo.utiltyx.com/api for all APIs

Example:
http://grideyedemo.utiltyx.com/api/login
http://grideyedemo.utiltyx.com/api/logout

/login

[POST]-> JSON
{uname:'user name', 'pwd':'password'}
return: {'status':1}

for development& testing use:
{uname:'admin', 'pwd':'12345'}

/logout

[POST]

Dashboard

/traffic/<start_date>/<end_date>

[GET]
return: JSON array

example:/traffic/2022-01-01 00:00:00/2022-01-02 00:00:00

/devices_location

[GET]
return: [{'name':'sensor1', 'lat': '40.71727401', 'long':'-74.00898606'}]

/communications

[GET]
return: [{'source': '192.168.1.10', 'dest':'192.168.1.15', 'dport': 5000, 'int':'1026'}, {'source': '192.168.1.12', 'dest':'192.168.1.15', 'dport': 9010, 'int':'2000'}]

/recentthreats

[GET]
return: [{'severity': 'high', 'timestamp': '2022-05-21 14:11:09', 'alert_id': 11, 'signature':'ENIP/CIP - Rockwell, Remote Mode Change Attempt from Unauthorized Client', 'src_ip': '192.168.1.10', 'dest_ip': '192.168.1.15', 'dest_port':5000}]

*** Connected devices

/devices_map

[GET]
return: {'links':[{'source':'192.168.1.10', 'destn':'192.168.1.15', 'network':'Sesnor1'}], 'devices':['192.168.1.10', '192.168.1.15']}

/devices_map/{filter}

filter: online, offline
[GET]
return: {'links':[{'source':'192.168.1.10', 'destn':'192.168.1.15', 'network':'Sesnor1'}], 'devices':['192.168.1.10', '192.168.1.15']}

Threats

/threats/{page}

[GET]
example: /threats/0, /threats/10, /threats/20
return: [{'severity': 'high', 'timestamp': '2022-05-21 14:11:09', 'alert_id': 11, 'signature':'ENIP/CIP - Rockwell, Remote Mode Change Attempt from Unauthorized Client', 'src_ip': '192.168.1.10', 'dest_ip': '192.168.1.15', 'dest_port':5000}]

/threat_description/{threat_id}

[GET]
example: JSON

/marksafe/{alert_id}

[GET]
alert_id: /threats-> alert_id
return: {'status': 1 or 0}

/reportfp/{alert_id}

[GET]
alert_id: /threats-> alert_id
return: {'status': 1 or 0}

Settings

/threat_det_policies

[GET]
return: JSON

/threat_det_policies/update

[POST]-> JSON
return: {'status': 1}

/sensors

[GET]
return: [{'name': 'sensor1', 'last_seen': '2022-05-21 14:11:09', 'first_seen': '2022-05-21 14:11:09', 'key':'f50ec0b7-f960-400d-91f0-c42a6d44e3d0', 'pwd':'&BYVE02ed'}]

/sensor/add

[POST]-> JSON
{'name': 'sensor name'}

/sensors/delete/{key}

[POST]
sensor_id: /sensors-> key
return: {'status':1}

/alerts_forwarding/siem

[GET]
return: [{'name': 'ARCSIEM', 'server_url': '192.168.0.245', 'protocol': 'TCP', 'port': '514', 'format': 'JSON'}]

/alerts_forwarding/siem/add

/alerts_forwarding/siem/update

[POST]->JSON
{'name': 'ARCSIEM', 'server_url': '192.168.0.245', 'protocol': 'TCP', 'port': '514', 'format': 'JSON'}
return: {'status':1}

/alerts_forwarding/siem/delete/{name}

[POST]
name: /alerts_forwarding/siem -> name
return: {'status':1}

/alerts_forwarding/email

[GET]
return: [{'name':'#001','display_name':'utlty-alert','to':'secalerts001@techions.net', 'from':'alert@utiltyx.com', 'add_recipients':['INFOSEC@techions.ne']}]

/alerts_forwarding/email/add

/alerts_forwarding/email/update

[POST]->JSON
{'name':'#001','display_name':'utlty-alert', 'to':'secalerts001@techions.net', 'from':'alert@utiltyx.com', 'add_recipients':['INFOSEC@techions.ne']}
return: {'status':1}

/alerts_forwarding/email/delete/{name}

[POST]
name: /alerts_forwarding/email-> name
return: {'status':1}

/alerts_forwarding/api

[GET]
return: [{'name':'response-ticket', 'server_url':'192.168.0.240', 'api':'a4db08b7-5729-4ba9-8c08-f2df493465a1','method':'POST', 'format':'JSON', 'useragent':'utiltyx-agent'}]

/alerts_forwarding/api/add

/alerts_forwarding/api/update

[POST]
{'name':'response-ticket', 'server_url':'192.168.0.240', 'api':'a4db08b7-5729-4ba9-8c08-f2df493465a1','method':'POST', 'format':'JSON', 'useragent':'utiltyx-agent'}

/alerts_forwarding/api/delete/{name}

[POST]
name: /alerts_forwarding/api-> name
return: {'status':1}

/users

[GET]
return: [{'name':'admin','email':'mark.taylor@techions.net', 'role': 'org-admin', 'permissions':['modify configurations', 'manage users', 'manage policy', 'report FP']}]

/users/add

[POST]-> JSON
{'name':'admin','email':'mark.taylor@techions.net', 'pwd':'388g8g8hg', 'role': 'org-admin', 'permissions':['modify configurations', 'manage users', 'manage policy', 'report FP']}
return: {'status'1}

/users/delete/{email}

[POST]
return: {'status':1}

/sys_settings

[GET]
return: {'update_auto_install': 1}

/sys_settings/update

[POST]-> JSON
{'update_auto_install': 1, 'restart': 0}
return: {'status':1}