

CHOO CHOO, NETWORK TRAIN

THE ONE TO RULE YOUR PERIMETER

MARTIN HRON

 **black hat**
EUROPE 2022

TRAIN OPERATOR

NAME

MARTIN HRON

ALIAS

THINKCZ

OCCUPATION

SECURITY RESEARCH

AFFILIATES

INDEPENDENT

AVAST

2K GAMES

SODATSW



DIAGNOSES

COFFEE ADDICT

THINGS BREAKER

OCD

SKILLS

LOW-LEVEL

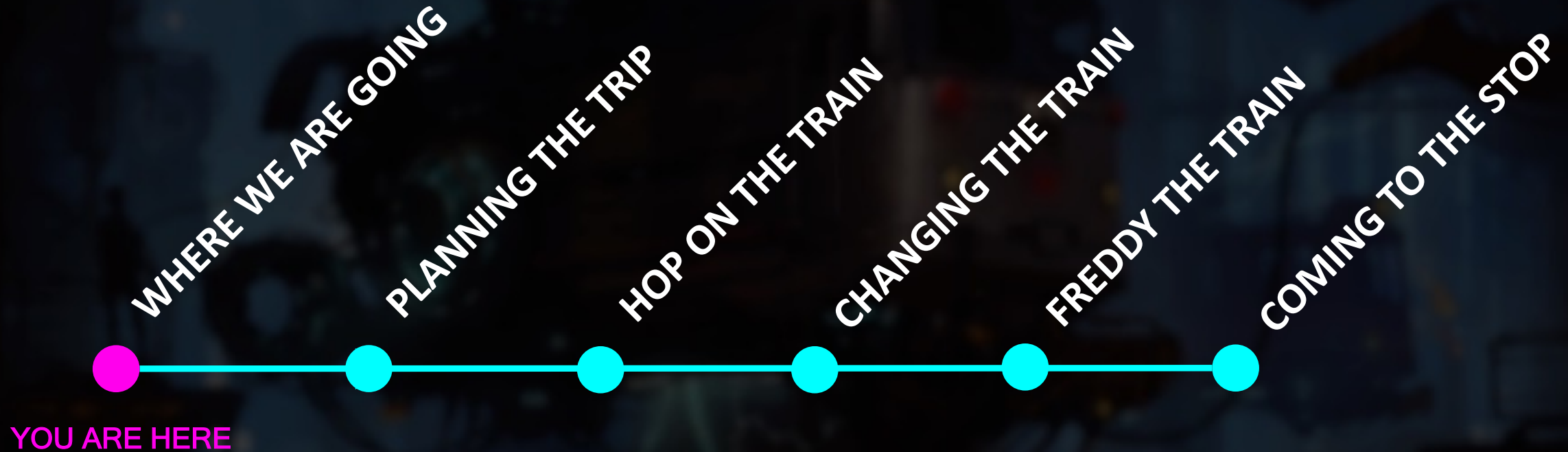
HARDWARE

REVERSING

COFFEE MACHINES

DIAL-UP AND BBS

WHERE WE ARE GOING



WHERE WE ARE GOING

A computer lets you make more mistakes faster than any invention in human history - with the possible exceptions of handguns and tequila.”

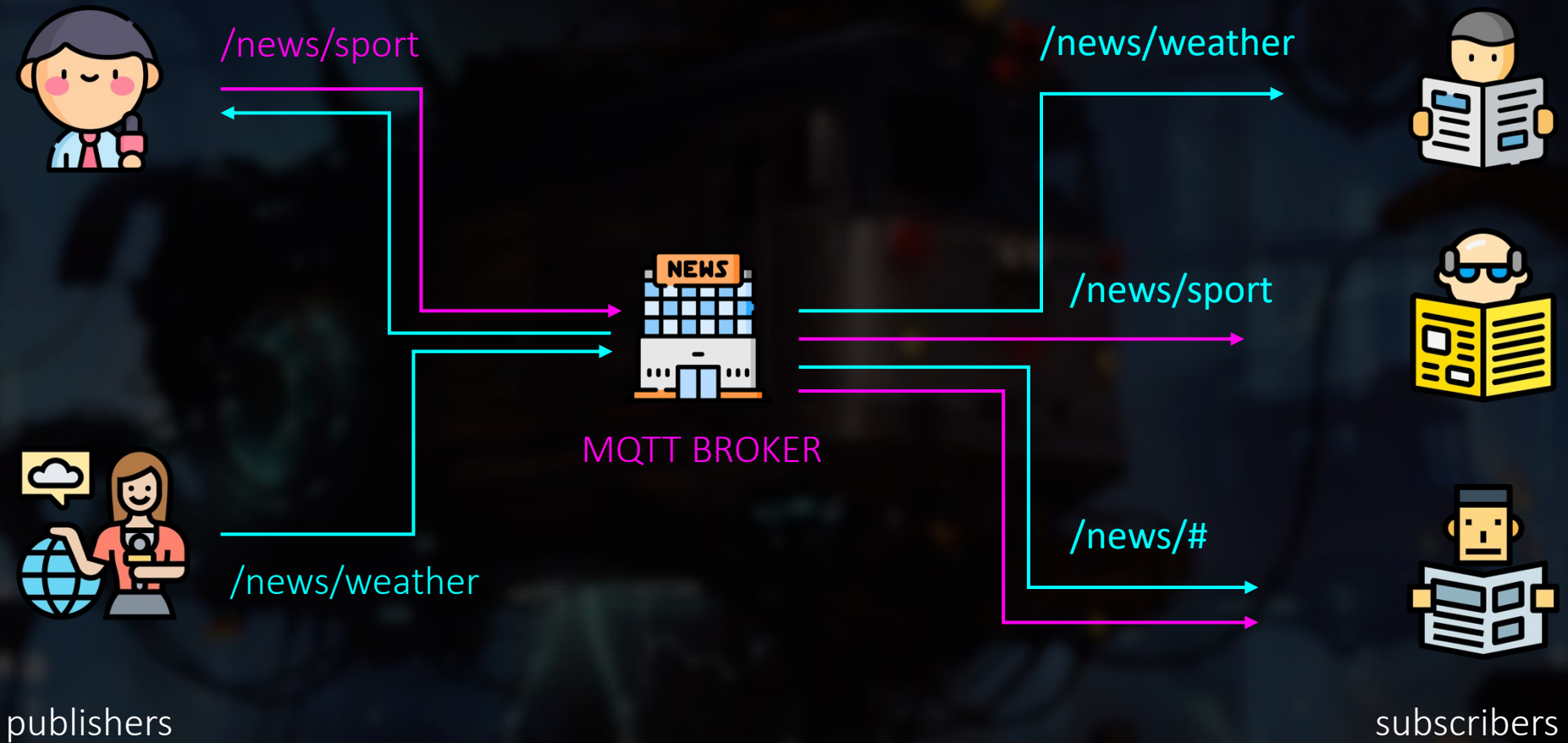
Mitch Ratliff

PLANNING THE TRIP

PLANNING THE TRIP



MQTT NAIVE MODEL



MQTT BASICS

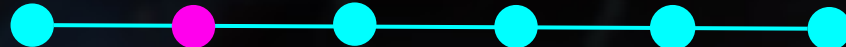
- publisher - subscriber model
- payload agnostic
- topics can be organized in a tree like structure
- when subscribing, wildcards # and + can be used
- usually operates through TCP on port 1883 and 8883 for TLS
- supports the last will and retained topics

MQTT BROKERS

- the most famous and used is **mosquitto** (over 80%)
- supports **ACL** lists
- plaintext **TCP**, **TLS** or **WS**
- username, password, certificate, client identification
- multiple listeners with separate configs

WHEN OCD KICKS IN

PLANNING THE TRIP





PRIVACY AND SECURITY FANATIC

By [Ms. Smith](#), CSO | AUG 20, 2018 8:41 AM PDT

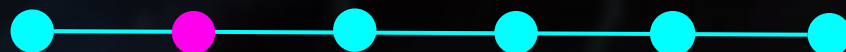
About |

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

NEWS

32,000 smart homes can be easily hacked due to misconfigured MQTT servers

Thanks to MQTT servers which are either misconfigured or not protected with a password, it is easy peasy to hack a smart home.



OUT-OF-THE-BOX PROBLEM

Devices and SW designed with convenience in mind more than security, leads to the situation where more than 60% installations of MQTT servers have never been set-up and left with default credentials

PLANNING THE TRIP




```
root@localhost:~#
```

```
0 root@74.208.27.198
```

```
→ / mosquitto_sub -h 74.208.27.198 -t '$SYS/#'
```

```
1 /
```

THE PROBLEM



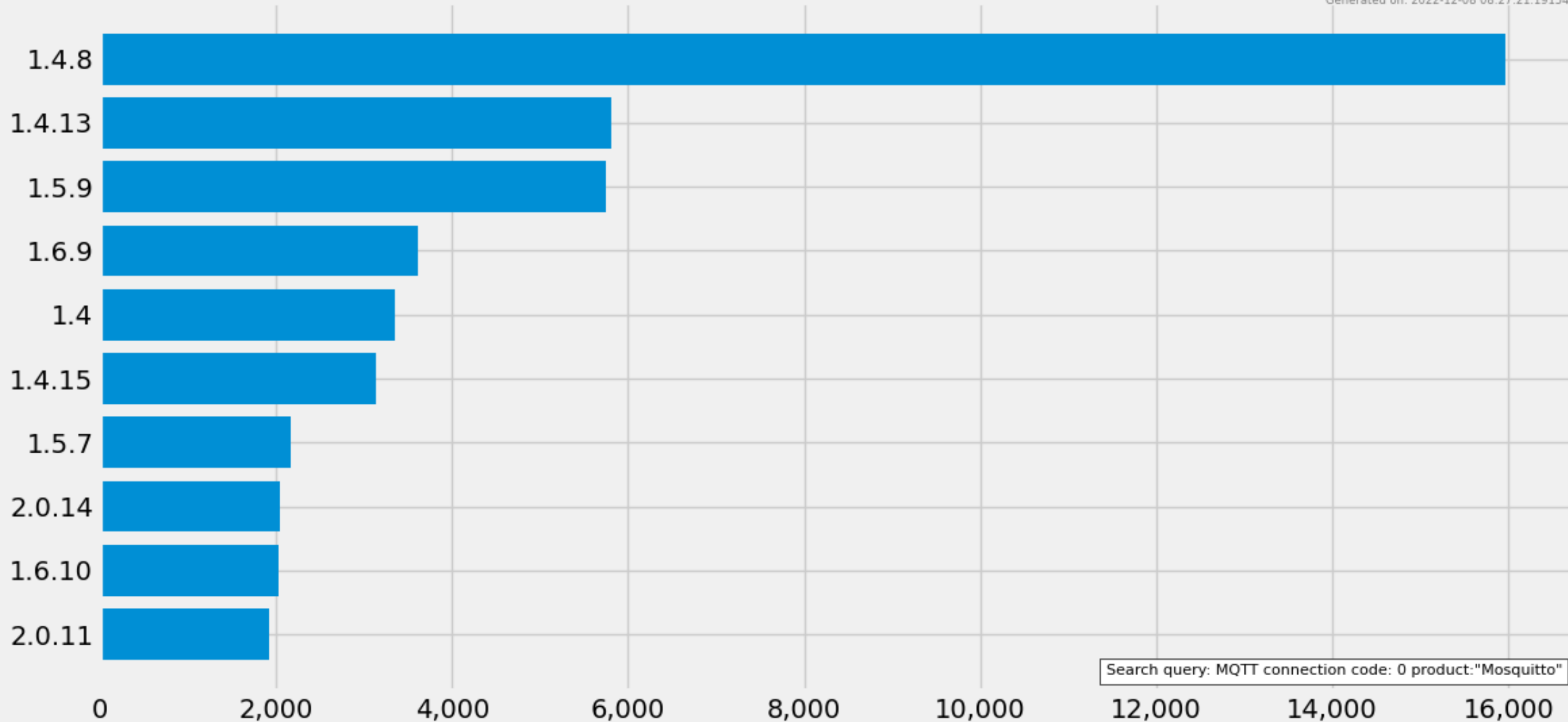
```
# defaults to true  
# for version < 2.0  
# allow_anonymous false
```



```
# defaults to false  
# for version >= 2.0  
# allow_anonymous false
```

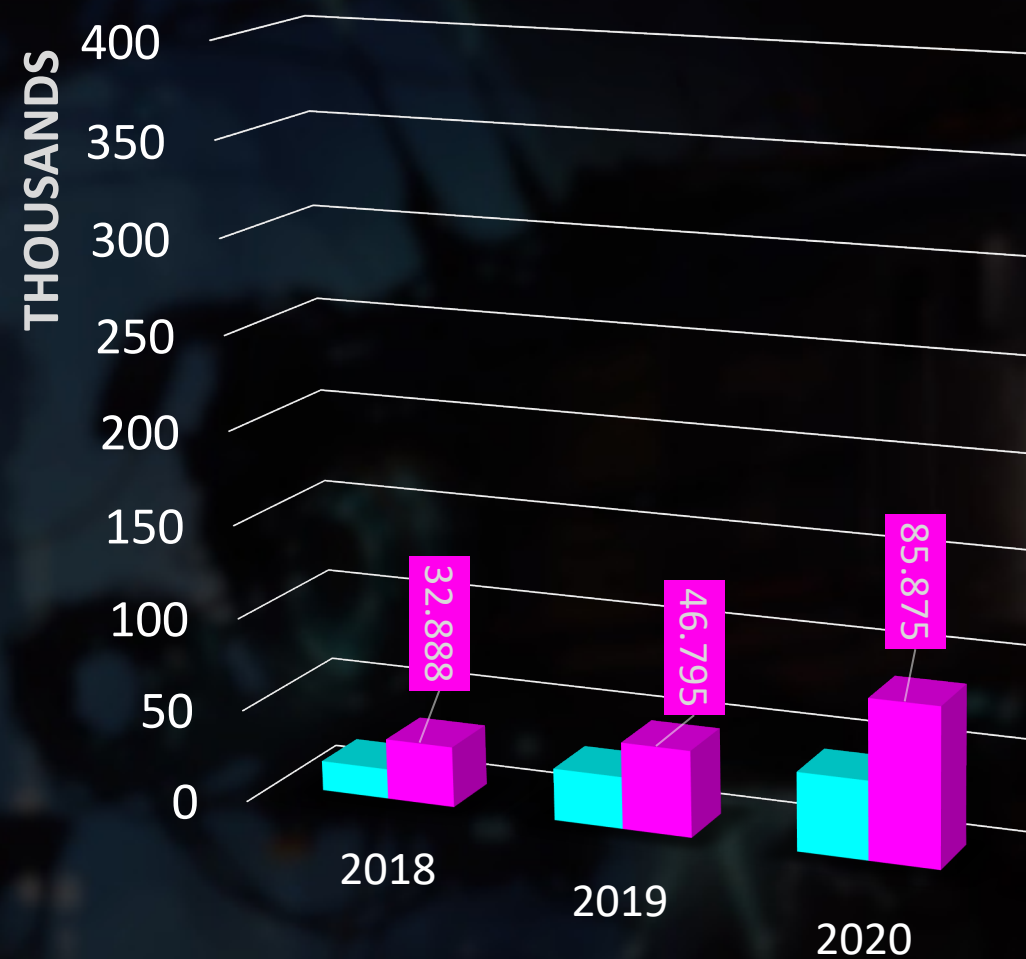
Top 10 Values for: version

Generated on: 2022-12-08 08:27:21.191545



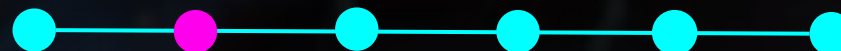
Search query: MQTT connection code: 0 product:"Mosquitto"

MQTT SERVERS OUT THERE

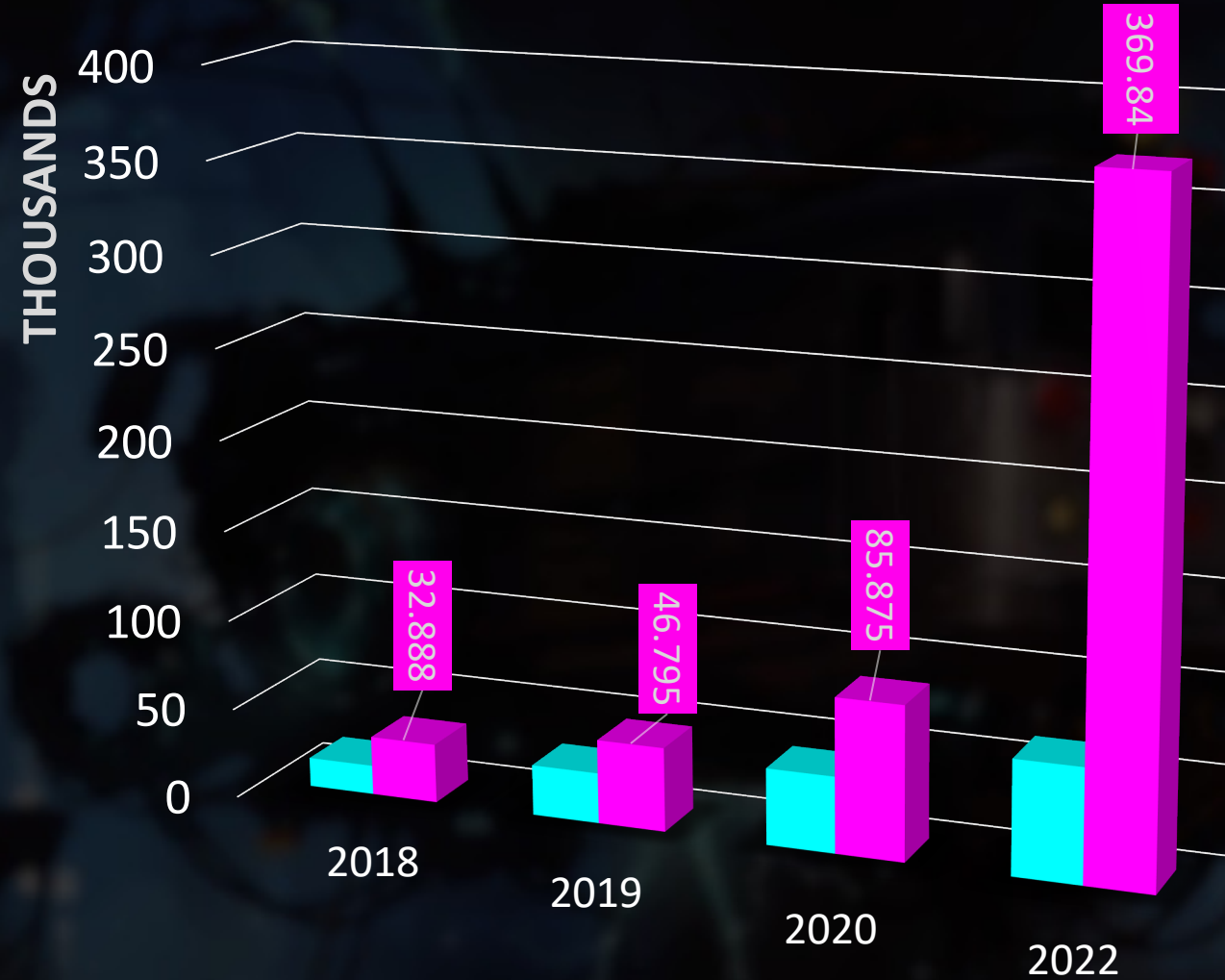


no password
protected

PLANNING THE TRIP



MQTT SERVERS OUT THERE



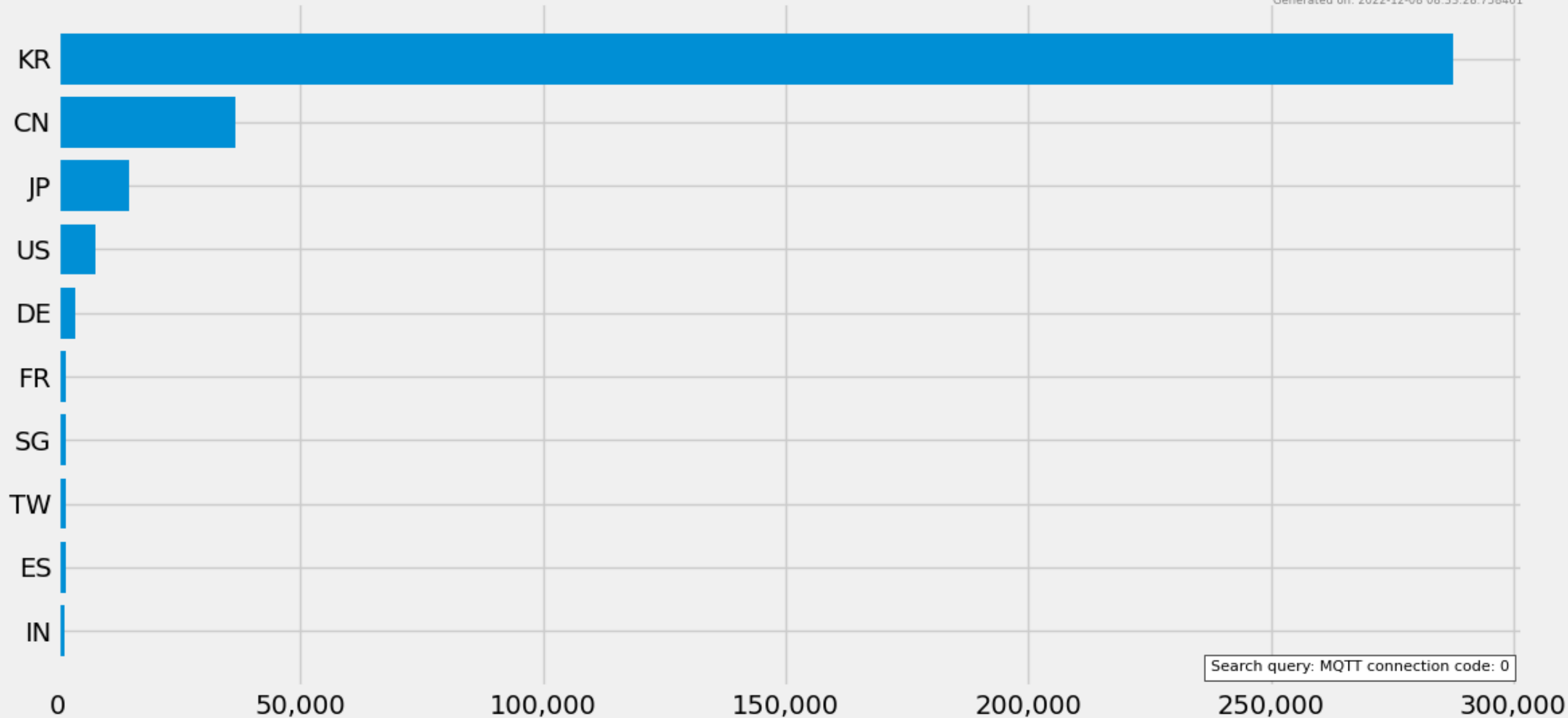
no password
password

PLANNING THE TRIP



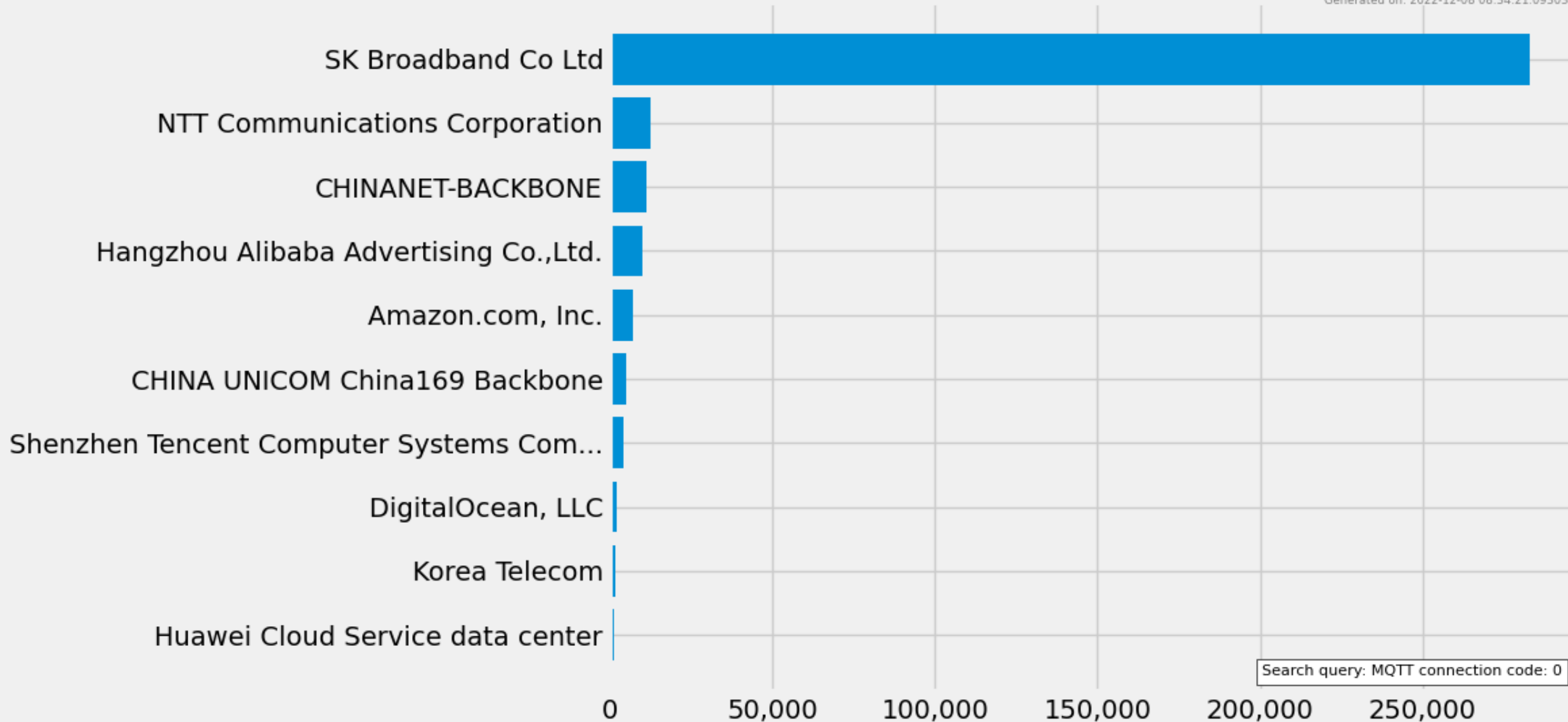
Top 10 Values for: country

Generated on: 2022-12-08 08:33:28.758401



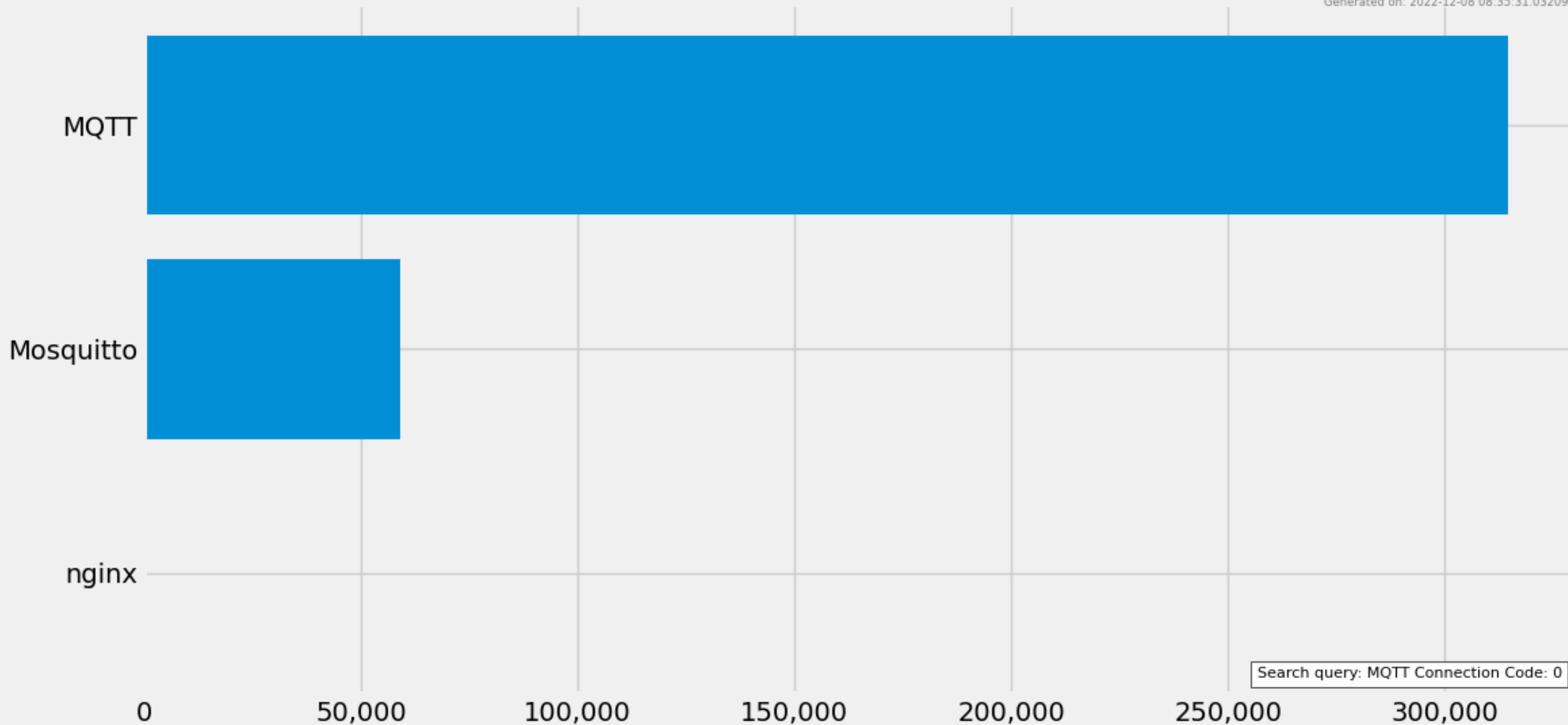
Top 10 Values for: isp

Generated on: 2022-12-08 08:34:21.093034

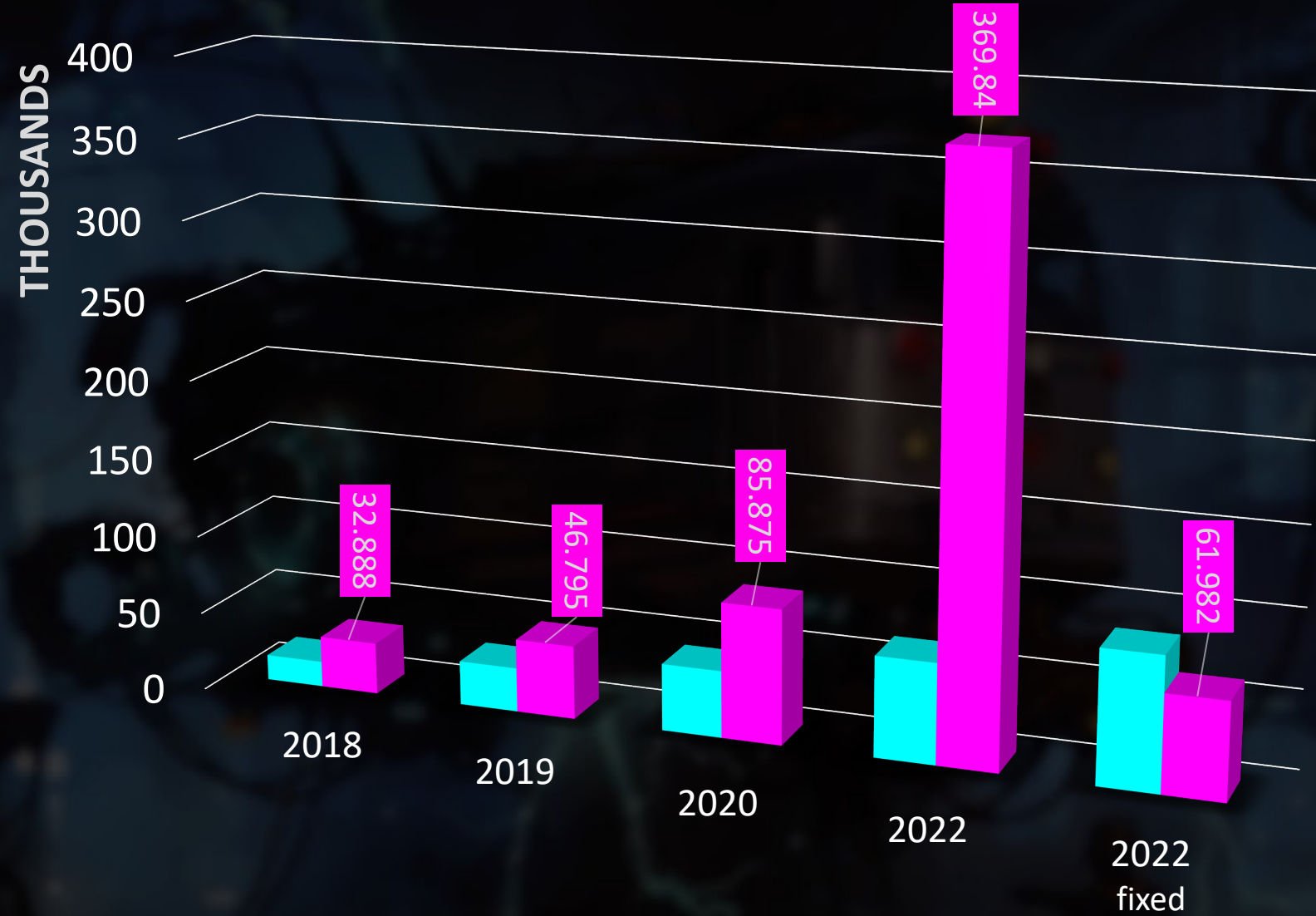


Top 10 Values for: product

Generated on: 2022-12-08 08:35:31.032099



MQTT SERVERS OUT THERE



no password
password

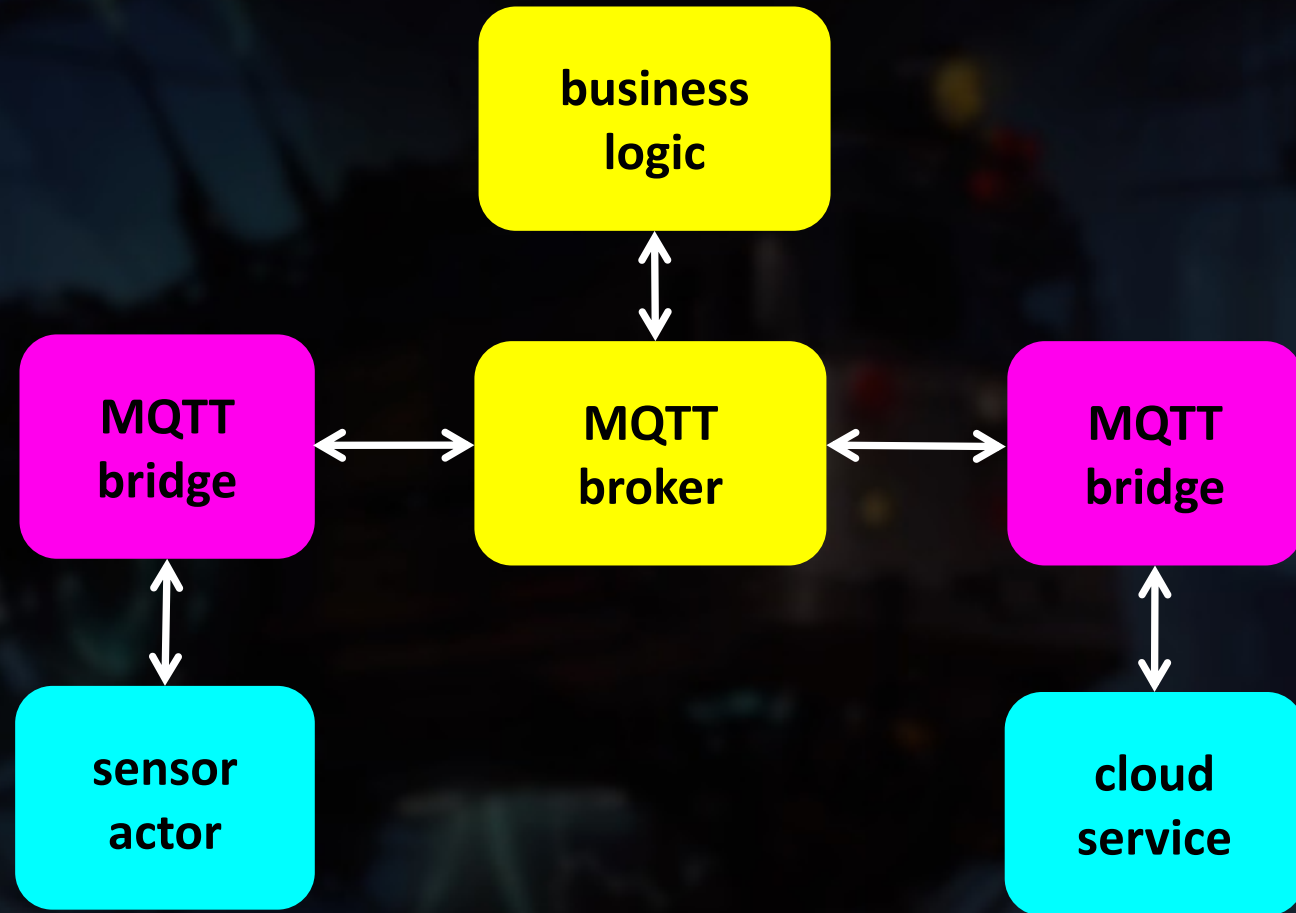
PLANNING THE TRIP

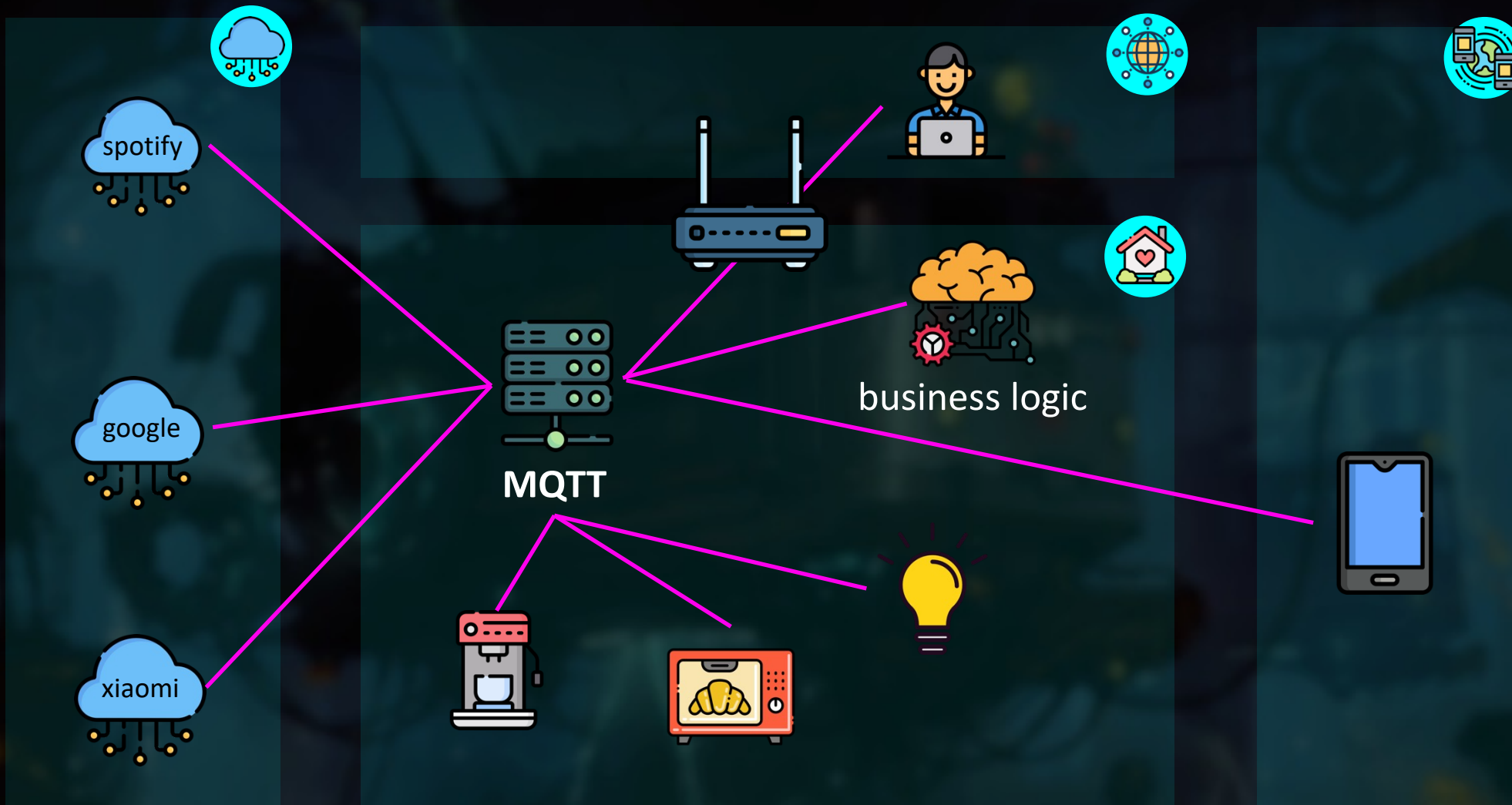


HOP ON THE TRAIN

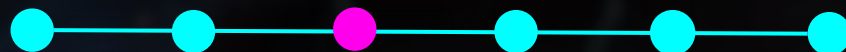
HOP ON THE TRAIN

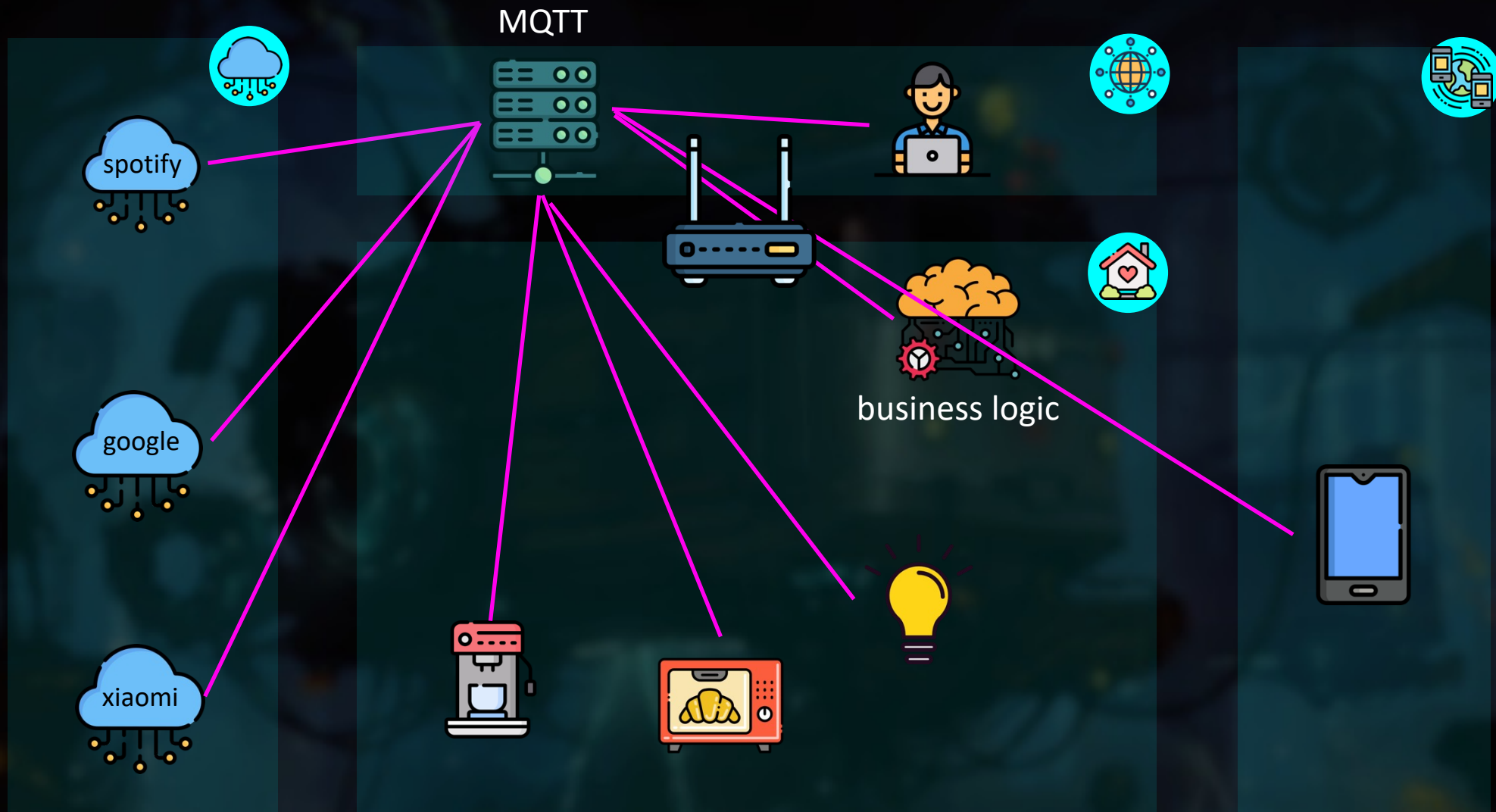






HOP ON THE TRAIN





HOP ON THE TRAIN



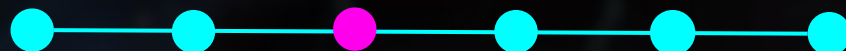
SET CREDENTIALS

USE ACL

USE TLS



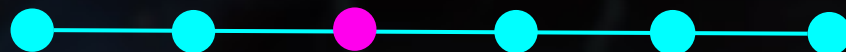
HOP ON THE TRAIN



imgdata/RBS_Kosanica/Camera_Indoor_axis_cam_device/application/x-tar



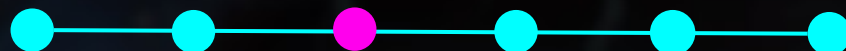
HOP ON THE TRAIN



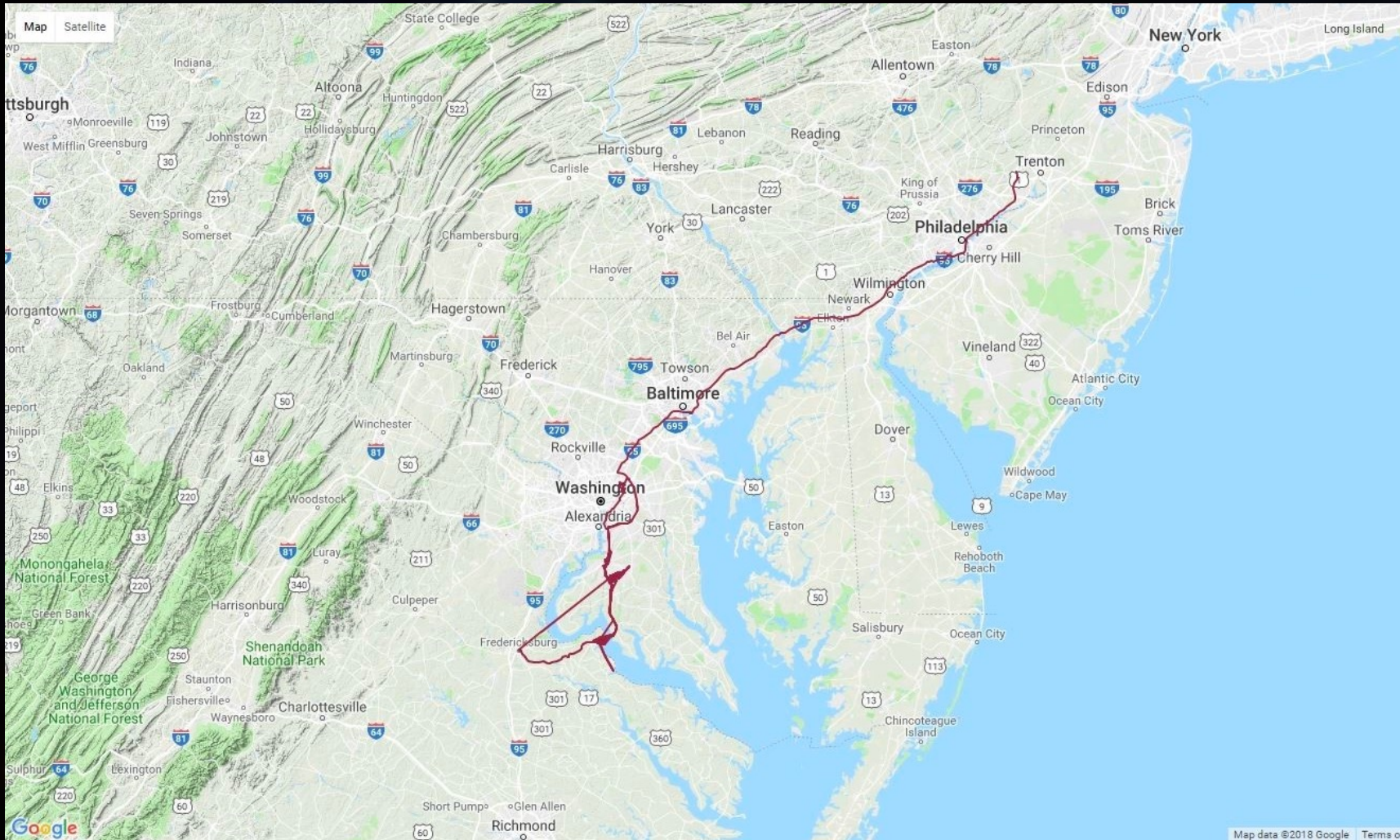
imgdata/RBS_Kosanica/Camera_Indoor_axis_cam_device/application/x-tar



HOP ON THE TRAIN



owntracks/#



OWNTRACKS

HOP ON THE TRAIN



metrics/exchange

ShowMe!

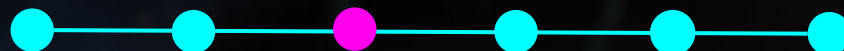


Pool Temp 82.4 51 seconds ago	Pool Pump Speed 50HZ 51 seconds ago	Pool Pump - Force on Temp 38 51 seconds ago	Bonus Room Temperature 76.21 13 seconds ago	Outdoor Light Level 1 51 seconds ago	Garage Freezer Temperature 0.0 51 seconds ago	Garage Temperature 87.0 51 seconds ago	Attic Floor Temperature 73.5 51 seconds ago
Attic Upper Temperature 69.8 51 seconds ago	Office Motion  51 seconds ago	Office Temperature 80.26 51 seconds ago	Office Humidity -2.46 51 seconds ago	Electric Blankets  May 21, 2018	Frank's Lamp  51 seconds ago	Kristi's Lamp  May 22, 2018	Master Bedroom Lights On 51 seconds ago
Office Small Lamp  May 22, 2018	Office Floor Lamp  May 24, 2018	Kitchen Cabinet Lights  33 seconds ago	Wine Bottle Lights  51 seconds ago	LR Xmas Tree Lights  42 seconds ago	US Xmas Tree Lights  51 seconds ago	Xmas Canvas 01  51 seconds ago	Xmas Canvas 02  51 seconds ago
Office Fan  51 seconds ago	Xmas Lights 03  51 seconds ago	Xmas Lights - Foyer  51 seconds ago	Landscape Lights - Front  51 seconds ago	Landscape Lights - Back  51 seconds ago	Pantry Lights  51 seconds ago	Pool Light  51 seconds ago	Pool Plumbing Freeze Protection  Apr 6, 2018
Pool Pump Temp	At Home	Garage Door	Allow GD Operation	US Occupancy	In Bed?	At Home	Dining Room Light



MQTT DASH

HOP ON THE TRAIN



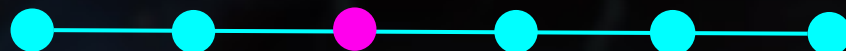
SET CREDENTIALS

USE ACL

USE TLS

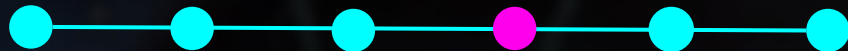


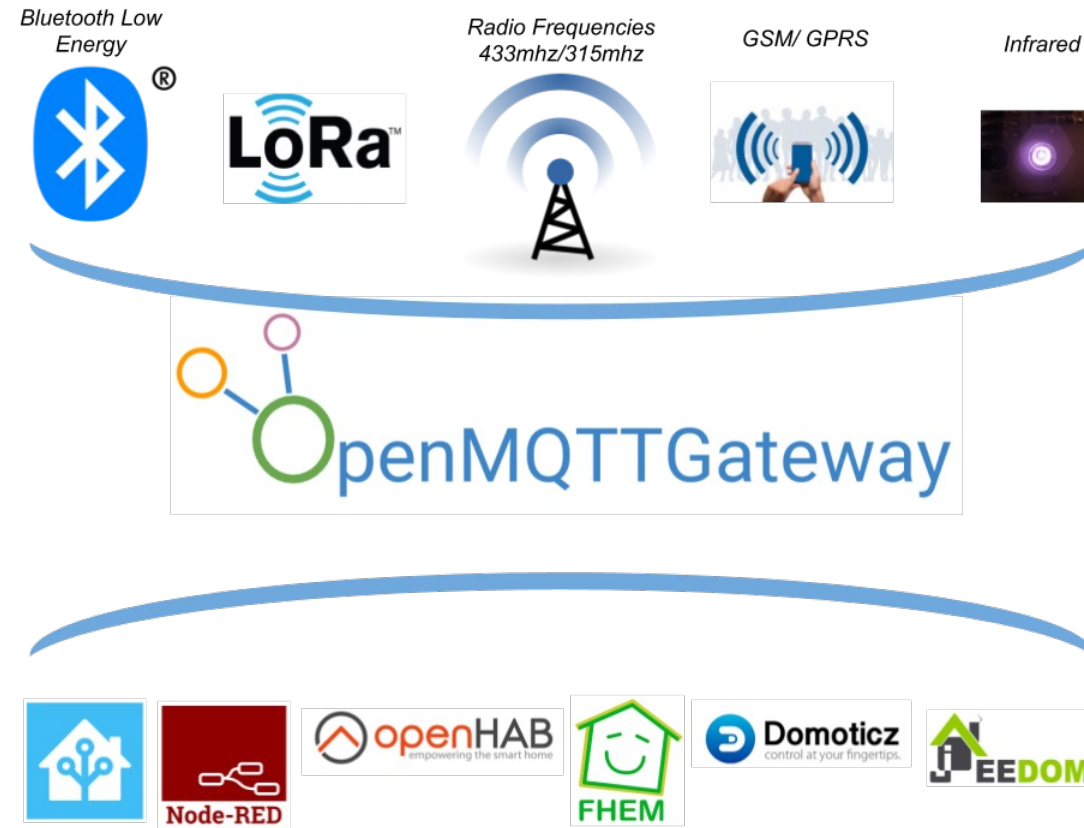
HOP ON THE TRAIN



CHANGING THE TRAIN

CHANGING THE TRAIN





Read/write BLE characteristics over MQTT (ESP32 only)

The gateway can read and **write BLE characteristics** from devices and provide the results in an MQTT message.

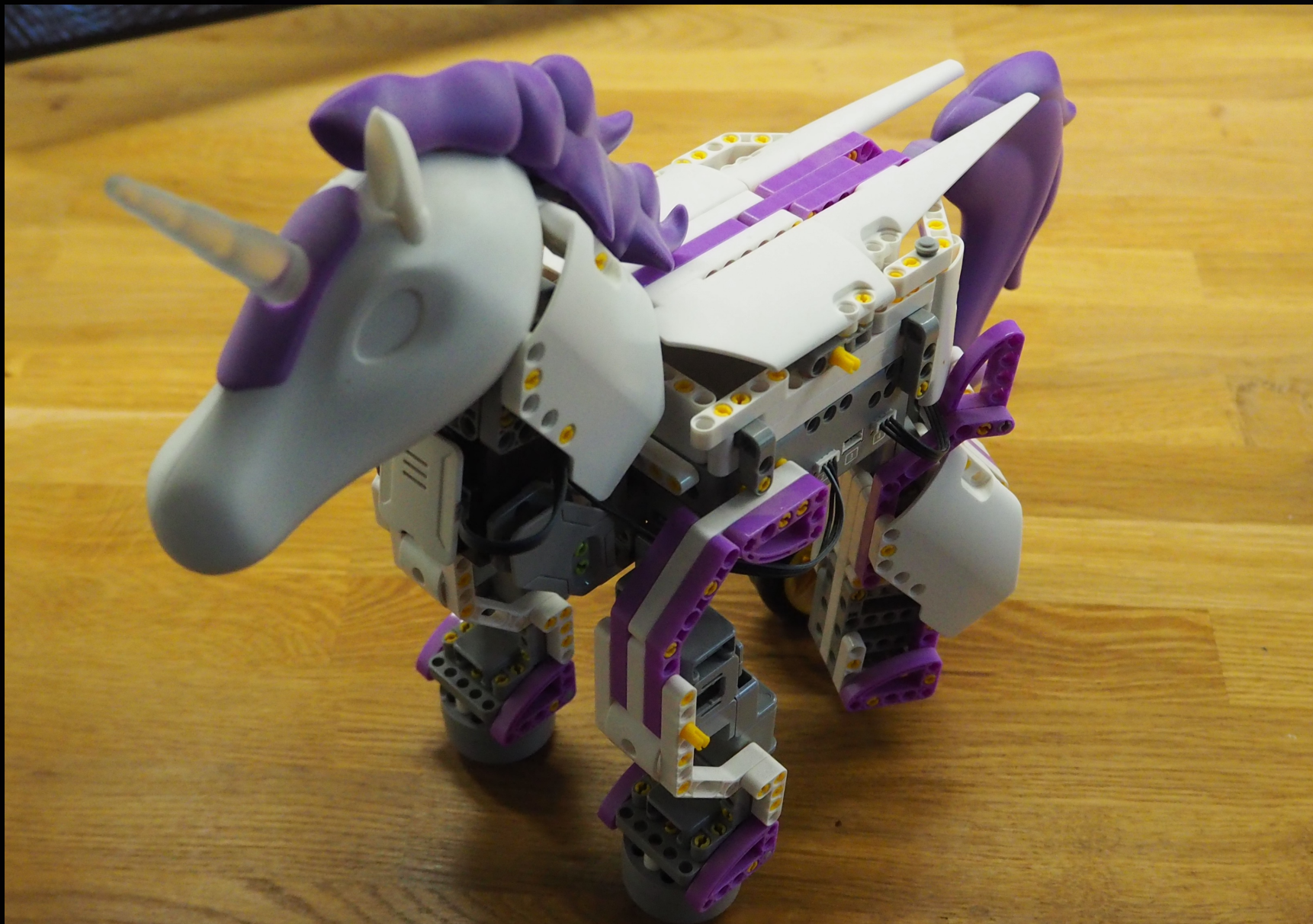
TIP

These actions will be taken on the next BLE connection, which occurs after scanning and after the scan count is reached, [see above to set this](#). This can be overridden by providing an (optional) parameter **"immediate": true** within the command. This will cause the BLE scan to stop if currently in progress, allowing the command to be immediately processed. All other connection commands in queue will also be processed for the same device, commands for other devices will be deferred until the next normally scheduled connection.

Note Some devices need to have the MAC address type specified. You can find this type by checking the log/MQTT data and looking for "mac_type". By default the type is 0 but some devices use different type values. You must specify the correct type to connect successfully. To specify the MAC address type add the parameter **"mac_type"** to the command. For example **"mac_type": 1** to connect with a device with the MAC address type of 1.

Example write command

```
1 mosquitto_pub -t home/OpenMQTTGateway/commands/MQTTtoBT/config -m '{  
2   "ble_write_address":"AA:BB:CC:DD:EE:FF",  
3   "ble_write_service":"cba20d00-224d-11e6-9fb8-0002a5d5c51b",  
4   "ble_write_char":"cba20002-224d-11e6-9fb8-0002a5d5c51b",  
5   "ble_write_value":"TEST",  
6   "value_type":"STRING",  
7   "ttl":4,  
8   "immediate":true }'
```

BREED

UNICORNBOT

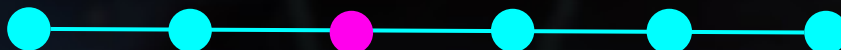
SPECIAL SKILLS

RGB HORN

SERVOS

SPEAKS BLE

CHANGING THE TRAIN





0 ~

martin at bumblebee in ~ 22-12-05 - 14:51:15
[py3]-o

```
[>] home/OpenMQTTGateway_BH/LWT  
online  
[>] home/OpenMQTTGateway_BH/version  
version_tag  
[>] home/OpenMQTTGateway_BH/SYSToMQTT  
{"uptime":371,"version":"version_tag","freemem":144624,"mqttport":  
:"1883","mqttsecure":false,"freestack":4660,"rssi":-14,"SSID":"demo-w  
ifi","BSSID":"D6:CA:6D:D0:89:1D","ip":"192.168.88.252","mac":"24:6F:2  
8:25:13:34","lowpowermode":0,"btqblk":0,"btqsum":61,"btqsnd":61,"btq  
avg":1,"interval":55555,"scanbcnct":10,"scnct":0,"modules":["BT"]}
```

1 python3

2 ~

Open source firmware for ESP8266 devices



Total local control with quick setup and updates.

Control using MQTT, Web UI, HTTP or serial.

Automate using timers, rules or scripts.

Integration with home automation solutions.

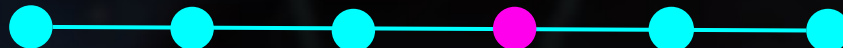
Incredibly expandable and flexible.



downloads 5.4M license GPL-3.0 chat 848 online donate PayPal

For OTA updates please use the new server <http://ota.tasmota.com/tasmota> and <http://ota.tasmota.com/tasmota32>

Download [Tasmotizer v1.1c](#) to use the new OTA server during flashing.



Tasmota Supported Devices Repository

Recently added:



AZzardo 10W RGB CCT Bulb AZ3213



AZzardo Led Vintage CCT Bulb AZ3210



Petoneer Smart Dot Cat Toy TY011 - DIY Replacement



Swisstone SH 310 CCT Bulb SH 310

2528 supported devices submitted by you!

Devices by electrical standard:



Light Bulbs by base:



See [world map of plugs](#) and [light bulb base list](#) for more information.

GroupTopic

Having two devices with the same topic allowed for MQTT commands to be sent once to make the devices act in conjunction. That inspired a third topic called GroupTopic. Devices with the same GroupTopic will all listen to that GroupTopic and react to the same MQTT command sent to it. You can use this to take global actions like **updating firmware on all devices** or split up devices into different groups using a unique GroupTopic for each group.



Default GroupTopic is tasmotas



Connections

Blackhat-demo

mqtt://demoserver:1883/

BlackHat-tasmota

mqtt://hidden-server-01:1883/

MQTT Connection

mqtt://hidden-server-01:1883/

Name

BlackHat-tasmota

Validate certificate ☒

Encryption (tls) ☐

Protocol

mqtt://

Host

hidden-server-01

Port

1883

Username

Password



DELETE



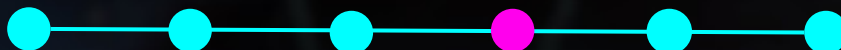
ADVANCED



SAVE



CONNECT



WebSend

Send a command to Tasmota host over http. If a command starts with a `/` it will be used as a link.

```
[<host>:<port>,<user>:<password>] <command>
```

`<host>` = hostname or IP address.

`<port>` = port for the device if not the default `80`

`<user>` = enter username of the device you're sending the command to

`<password>` = enter password of the device you're sending the command to

`<command>` = command and payload

example 1: `[<ip>] POWER1 ON` sends `http://<ip>/cm?cmd=POWER1 ON`

example 2: `WebSend [myserver.com] /fancy/data.php?log=1234` sends

`http://myserver.com/fancy/data.php?log=1234`

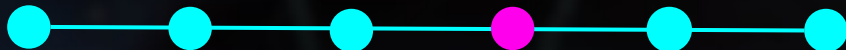
root@acme:~#

0 root@92.38.163.119

martin at bumblebee in ~ 22-12-05 - 10:43:43

1 ~

CHANGING THE TRAIN





FREDDY THE TRAIN

FREDDY THE TRAIN



OtaUrl

Display current OTA URL

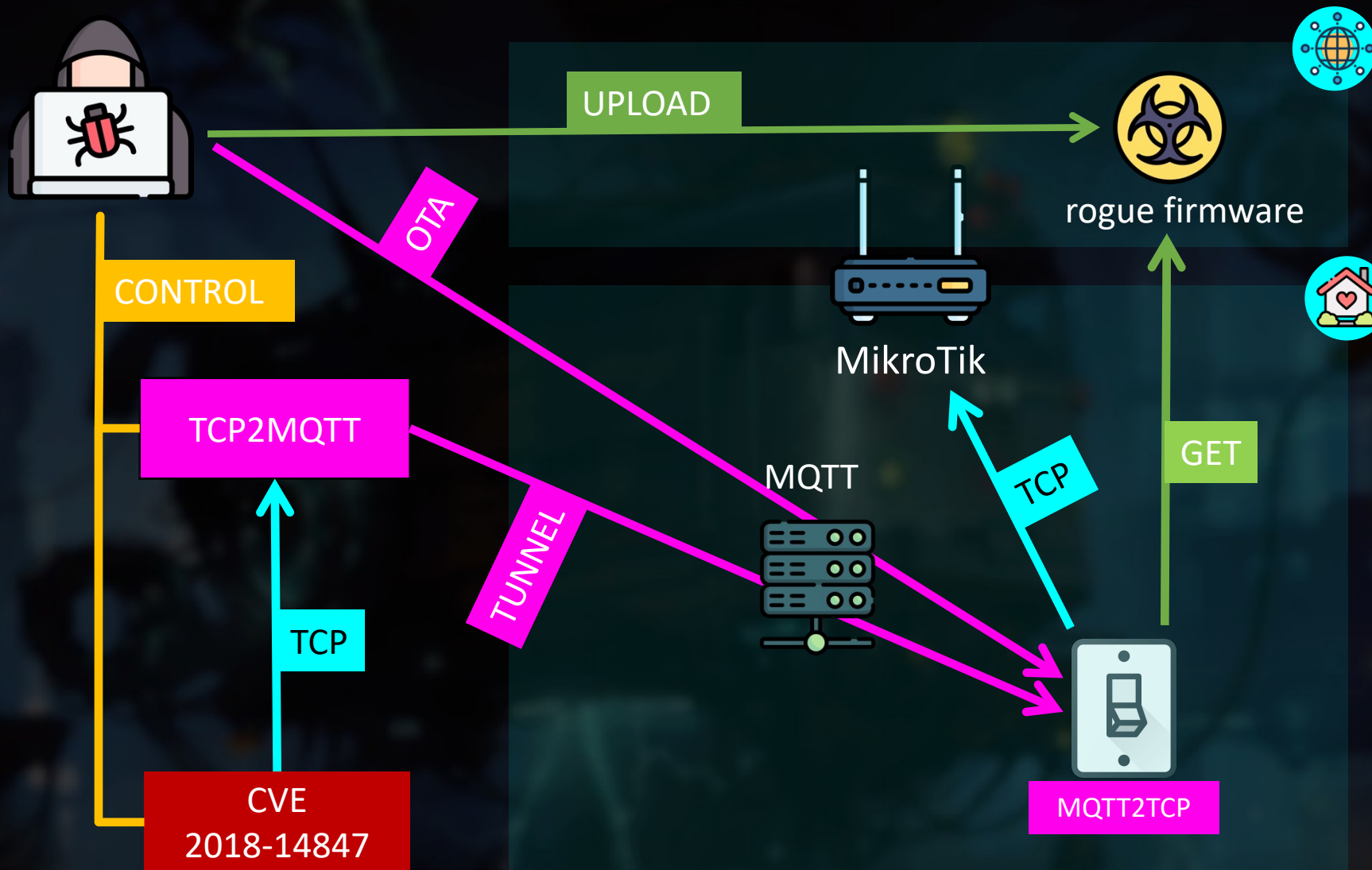
`1` = Reset OtaUrl to firmware default

`url` = set address for OTA (100 char limit)

Upgrade

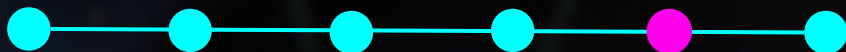
`1` = download firmware from `OtaUrl` and restart

`<value>` = download firmware from `OtaUrl` if `<value>` is higher than device version





FREDDY THE TRAIN

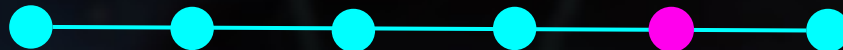


G+ xdrv_01_webserver.ino 4, M ●



tasmota > G+ xdrv_01_webserver.ino

```
3409 | &CmndEmulation,  
3410 | #endif  
3411 | #ifdef USE_SENDMAIL  
3412 | &CmndSendmail,  
3413 | #endif  
3414 | &CmndWebServer, &CmndWebPassword, &CmndWeblog, &CmndWebRefresh, &CmndWebSend, &CmndWebColor,  
3415 | &CmndWebSensor, &CmndWebButton, &CmndCors, &CmndTCPConnect, &CmndTCPSend, &CmndTCPClose };  
3416 |  
3417 | /*****  
3418 | * Commands  
3419 | *****/
```



root@rogue:~#

[>] tele/demo-switch/LWT
Online

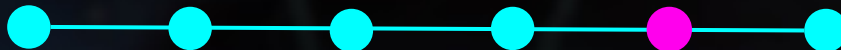
0 root@92.38.163.119

2 python

martin at bumblebee in ~ 22-12-05 - 11:24:01

1 ~

FREDDY THE TRAIN



```
[martin at bumblebee in ~ 22-12-05 - 11:43:30  
[py3]-o
```

```
[>] tele/demo-switch/LWT  
Online
```

0 ~

2 python

```
[martin at bumblebee in ~ 22-12-05 - 11:46:21  
[py3]-o
```

1 ~

FREDDY THE TRAIN



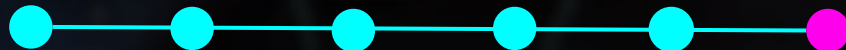
```
0 python
    username: nart
    password: HighScreen
[>] -----
    username: karel
    password: barel
[>] -----
    username: admin
    password: barel
[>] -----
```

FREDDY THE TRAIN



COMING TO THE STOP

COMING TO THE STOP



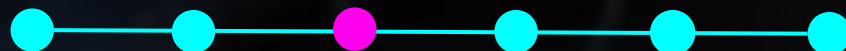
SET CREDENTIALS

USE ACL

USE TLS



HOP ON THE TRAIN



ALWAYS SECURE YOUR MQTT

HOP ON THE TRAIN

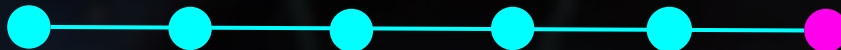


AS THE RISKS COULD BE "HIGH"

lab/webcams/feed01/snapshot_1m



COMING TO THE STOP



THANK YOU & QA

References:

Tools and PoC

https://github.com/thinkcz/tasmota_tcp2mqtt

Shodan.io

<http://shodan.io>

Tasmota repo

<https://tasmota.github.io/docs>

Welcome home! @Bsides Manchester

<https://www.youtube.com/watch?v=QX09BFAZqic>

MQTT Explorer

<https://mqtt-explorer.com/>

Unsplash images

<https://unsplash.com>

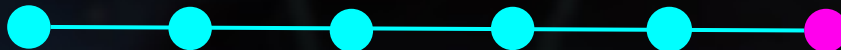
Alejandro Burdisio

<https://www.artstation.com/burda>



Martin Hron (@thinkcz)
martin@hron.eu

COMING TO THE STOP



BLACK HAT SOUND BYTES



DON'T DO DEFAULT...EVER

ALWAYS SECURE OTA CHANNEL

ALWAYS SETUP CREDENTIALS

CONTROL ACCESS AT THE HIGHEST
POSSIBLE GRANULARITY

COMING TO THE STOP

