FAQ

Can I use other sensors on my raspberry pi 3?

Yes, other sensors are accepted, however, the one documented here is a sense HAT.

Can I modify MicroAI™?

No. You may only modify X-code and Y-code. Which is essentially the input and output.

What are the requirements for running MicroAI™ on Windows?

MicroAI™ uses Python version 3.7.3 with these dependencies: NumPy, Psutil, waitress, dash, bottle, tablib, and paho-mqtt. For Redis, version 2.4 and above is sufficient.

Is there going to be a GUI for the MicroAI™ configuration, or will it always be command line/terminal based?

MicroAI™ is currently for use by developers in command line/terminal. No GUI is on the roadmap currently.

Is MicroAI™ supervised or unsupervised learning?

MicroAI™ uses semi-supervised learning. Model training does occur; however, it also learns on its own, in real time.

After you download the MicroAI™ SDK on your computer, do you need to run any installation?

No, once you have the file unzipped and your python dependencies installed, you can get started with MicroAI™.

If connecting to the device using SSH, do users need a VPN into a certain network for MicroAI™ to work?

No, the machine they are SSHing from just needs to be on the same network as the device they are running MicroAI™ on.

If I launch an attack simulation right after an attack has just completed, will the AI detect this?

It depends. However, it is probably best to wait 20 minutes before running another attack script so the device behavior can settle.

How far ahead of time can MicroAI™ forecast?

MicroAI™ predicts values one step ahead of the current value. This could be one second ahead or hours ahead based on the output frequency.

Will MicroAI™ be able to detect anomalies that happen over long periods of time?

This will depend on how long the AI model is trained, as well as, the frequency of change.

What happens if the IoT Security AI model is trained while an attack is occurring or while a backdoor has already been exploited?

It is pertinent that when the MicroAI™ model is being trained, there are no previous or currently exploited vulnerabilities. These will make the predictive analysis inaccurate.

For training, can MicroAI™ intake data that is not part of real time asset data? Such as industry standard levels over time or lifetime data of a similar asset?

Yes, MicroAI™ can intake historical data as part of the training dataset.

Can different parameters fed into MicroAI™ be given different weights?

Yes, using feature engineering capabilities, MicroAI™ can incorporate different weights of channel values for optimal predictive analysis.

Can IoT security detect any vulnerabilities that are being exploited outside of the device?

When running on an edge device, MicroAI™ can only detect vulnerabilities on the device level. Not the network and application levels.

What is the limit of devices or channels that can be on a single MicroAI™ deployment?

Currently, MicroAI™ supports 100's of channels being ingested from a single edge device. However, the EVK limits users to 6 channels.

Permission Denied. How do I get execution rights to an executable file?

Some users will experience a permission denied error when attempting to run the executable files in the demos. To remedy this, use the command `chmod +x executable_name_here`.