# **Updated Project Proposal**

**Objective**Develop Proof of Concept **EDR(Endpoint Detection and Response)** solution on Pico. 2 Picos will be involved, the 1st pico will be emulating a simple IoT device which will be monitored by the a 2nd pico. The 2nd pico will be the EDR that is monitoring the emulated IoT device's ram and flash memory for changes in configurations, voltage, etc.

A concrete example would be, detecting changes in the firmware of the emulated IoT device. The EDR will then send a reset signal as a response to prevent the anomaly from taking effect. Data of such anomaly will also be recorded and stored in an SD card. Data being monitored will also serve a web GUI for the viewing of data.

**Main Tasks:**

**Emulation of IoT on target pico aka pico1 (Darren)**

* simulation of a simple IoT taken from github  
  this device will be monitored by our proof of concept EDR which is another pico
* any program can be flashed into this pico as we are only concerned about its flash and RAM contents which will be dumped via SWD protocol

**Dumping flash/ram content from pico1 using pico2 (Ivan, Darren)**

* development of logic for dumping data from flash or ram of pico1 using SWD protocol to apply detection logic.
  + SWD initialisation and commands require specific bytes to be used and sent to target pico to read ram/flash contents.

**Detection using pico EDR aka pico2 (Ethan)**

* monitor data anomalies in the ram and flash. Data anomalies are detected via byte determining the byte contents that are dumped from target pico are normal.
* Examples are:
  + firmware changes which are not supposed to happen
  + determine if behaviour of bytes that are constantly changing are normal
  + etc

**Storing of data received (Hannah)**

* storing of data in a micro-SD card for auditing purposes  
  additional processing to make it compatible with log collectors (E.g syslog, etc)

**Web server and gui server on pico EDR (Casanas)**

* a simple web dashboard written in C for data to be displayed
* in our case, any data anomalies will be flagged onto a display
  + this is to simulate a very simple SIEM use case for an embedded system

**Flowchart**

A diagram of a flow chart

Description automatically generated

**Block Diagram**

A diagram of a computer hardware system

Description automatically generated