**Vulnerability Mangamenet System Requirement**

# Background:

Vulnerability management is one of the essential 8 recommended by the Australian government, and a key security control to track and monitor vulnerabilities of information technology assets. A vulnerability management system commonly, discovers network-connected services and enumerates hard hardware, firmware/software of discovered resources and correlates with a database of known bugs and vulnerabilities to a reporting dashboard that provides visibility for service owners to patch up or remediate issues under their own process flow (e.g. install a patch).

Here, we have investigated to discover which resources exist in the Redback company to consider when selecting specific vendors.

# IT Assets discovered as per handover documents:

Raspberry Pi (Bikes) with sensors:

* KICKR Headwind Bluetooth Fan
* Wahoo speed and Cadence Sensor
* Wahoo TICKER Heart Rate Sensor
* Wahoo KICKR smart trainer and Wahoo KICKR Clibm

User Access Channels:

* Mobile Apps (Android, IOS)
* User Browser
* Unity Software
* IoT CMS (Web Server)
* MQTT Broker (HiveMQ) receives data from bikes.
* MongoDB Database
* GCP (for data store and CMS, currently on Quintin’s private account)

CICD Pipeline is not started yet, however, DevOps team is currently working on Ansible and Python for code development.

# System Requirements (Scope):

Here are identified areas the system should monitor for vulnerabilities:

* As data is generated and stored in GCP, The database management in GCP needs to be monitored and be in the scope.
* There is infrastructure such as firewalls, DNS, Web service, and so on provisioned in GCP which also need to be monitored and scanned periodically for vulnerabilities.
* There are applications and codes developed or under development in which VM is good to have a scanning tool for code analysis testing before code deployments and to be available for integration into CICD pipeline.
* Reported dashboard should be able to be visible for service owners as well as periodic reports or incidents generated to communicate discovered vulnerabilities with service owners.