# Sophos MDR – Hiring Coding Project (Ruby)

## Story

You’ve inherited a proof of concept for an Osquery fleet manager and it needs to be updated to production quality. It should validate the enrollment secret, generate a node key, and distribute the configuration based on the node key.

## Description

Write a simple Osquery fleet manager in Ruby that implements the Enrollment and Configuration APIs.Osquery should be able to enroll to the server using a “simple shared secret enrollment” and the server should return the Osquery configuration. This project requires 2 HTTP POST API endpoints to be implemented.

POST /enroll

POST /configuration

## Documentation

<https://osquery.readthedocs.io/en/stable/deployment/remote/#remote-server-api>

## Resources

### Osquery Binaries

Below are the Osquery binaries that can be used for this exercise. Use chmod to make them executable on MacOS or Linux.

MacOS - <https://s3-us-west-2.amazonaws.com/darkbytes-binaries/osquery/db-darwin>

Linux - <https://s3-us-west-2.amazonaws.com/darkbytes-binaries/osquery/db-linux>

Windows - <https://s3-us-west-2.amazonaws.com/darkbytes-binaries/osquery/db-windows.exe>

### Osquery Flag File / Configuration

The “osquery\_client” folder includes the Osquery flag file and the “server\_code” folder includes the Osquery configuration that the server should return from the “POST /configuration” API endpoint.

### Osquery Commands

The relevant command should be executed in the same directory as the flag file and secret file.

./db-darwin --flagfile db.flags --config\_dump

./db-linux --flagfile db.flags --config\_dump

./db-windows.exe --flagfile db.flags --config\_dump