Team 3
Team members: Aidan Curley, Kaoru Kitamura, Ian Wolloff
Tutor: Dr Cathryn Peoples
Date: May 2022

Criteria	Level	Comments
Knowledge and under-standing of the topic / issues under consideration (30%)	Excellent – Distinction	Good awareness of the domain. Good attention to gathering the domain-specific characteristics. Sensors which the application focuses on include: ● Oxygen ● Radiation ● Carbon dioxide Setup according to a master-slave config. A number of VMs have been created to achieve system redundancy. There is an opportunity to consider what the implication of this might be in terms of increasing the attack surface. Data replication feature. Design considered from the perspective of OWASP proactive controls.
Application of knowledge & understanding (30%)	Outstanding – Distinction	Priorities related to security include: ● High availability ● Secure ○ Fernet, pyjwt, werkzeug, Flask limiter ○ Data encoded at rest and in transit ○ Authentication required into system ● Data storage ● Operated from defined locations Solution corresponding with OWASP proactive controls JWT tokens have a one-hour lifespan, but are reconfigurable on demand. Shows good consideration of session control. Flask login to protect particular endpoints Impressive testing procedures written: ● Acceptance tests ● Authentication login tests ● Unit tests 2 APIs deployed within the system: 1. API to handle user authentication 2. Database API – pushing data to and from the database. Uses the JWT tokens. Secure socket connection. Range of operating systems supported: ● Debian, Ubuntu, RedHat, Windows Server, Windows 10

		LDAP used. Excellent evidence of the required producer consumer capability. Each sensor runs on a separate thread. Thread data is communicated into Kafka, consumer polls the queue for content, and puts thread contents placed into database once retrieved. Numerous examples of try..catch to support exception handling.
Structure & Presentation (30%)	Excellent – Distinction	Careful control of the presentation to communicate the project work within the window of time available. Two out of the three team members were present for the demonstration. Excellent attention to structure and presentation throughout the code. Some opportunities to label some/all of the imported libraries. Have you applied PEP 8 Style Guide? https://peps.python.org/pep-0008/
Academic integrity (10%)	Outstanding – Distinction	Good information provided on the attempted API attacks. Opportunity for supporting your .ppt with references to academic literature. However, it should be noted that referencing dotted throughout the supporting document uploaded with the code. I also want to commend your academic behaviour throughout this module. I recognise that the team structure was not optimum, and you responded to that in a very professional way. Thank you.

Overall comments:

Positives:

- Excellent academic integrity and conduct throughout this module.
- Excellent range of technologies harnessed to support your implementation.
- Good evidence provided of the producer-consumer capability, as requested.
- A great testing process has been orchestrated for demonstrating system capability.

Points for development:

- There is a cost-benefit balance to be achieved when provisioning a secure solution. We want to ensure sufficient redundancy and replication across the system, however, we also want to ensure that the attack surface has been carefully considered. I believe it is fine to create the system with redundancy as you have, however, there may have been an opportunity to consider the implications of this on the extent of the attack surface, and to take some degree of proactive control associated with this.

- There may have been an opportunity to give a little more focus on the specific security angles, and identifying potentially suspicious behaviours e.g., large volumes of data being deleted within a short time or many log-in attempts from a particular IP address within a restricted period. An alert could be flagged in such a case.

Overall Grade: Excellent - Distinction