Edith Cowan University
School of Science

CSI2450 – IoT and OT Security

Assessment 2: Case Study Rubric

Marking Key/Rubrics:

Please read, understand and do your best to apply each of the criterion and the requirements to score a good grade.

Criterion	Needs Improvement 0% - 49%	Satisfactory 50% - 69%	Good – Excellent 70% - 100%
T1 – Introduction and Overview **(1% - 0.4 marks)**	Failed to provide an introduction and/or overview.	An introduction is provided including some of the following: An introduction of the presenter And Described the logical/conceptual setup diagram And Described the attacks and defensive measures using the diagram.	An introduction is provided including all the following: An introduction of the presenter And Described the logical/conceptual setup diagram And Described the attacks and defensive measures using the diagram.
T2 – MQTT Broker status	The status of the mosquitto service is not shown And/or The service is not running.	The status of the mosquittto service is shown And/or The service is running successfully.	The status of the mosquitto service is shown and The service is running successfully.
T3 – MQTT Publish-Subscribe **(5% - 2 marks)**	A Terminal window running the Publisher And/or A separate Terminal window running the Subscriber were not shown.	A Terminal window running the Publisher And/or A separate Terminal window running the Subscriber were shown partially.	A Terminal window running the Publisher And A separate Terminal window running the Subscriber were shown.
T4 – Network traffic capture and analysis **(5% - 2 marks)**	Evidence of Publisher-Broker communication was not shown And/or Evidence of Subscriber-Broker communication was not shown And/or Did not describe the evidence.	Evidence of Publisher-Broker communication was shown partially And/or Evidence of Subscriber-Broker communication was shown partially And/or Described the evidence to some extent.	Evidence of Publisher-Broker communication was shown And Evidence of Subscriber-Broker communication was shown And Described the evidence fully.

Criterion	Needs Improvement 0% - 49%	Satisfactory 50% - 69%	Good – Excellent 70% - 100%
T5 – FDI attack **(20% - 8 marks)**	A FDI attack against the Server (Mosquitto Broker) was not shown And/or The consequence of the attack was not shown And/or The consequence of the attack was not explained.	A FDI attack against the Server (Mosquitto Broker) was shown partially And/or The consequence of the attack was shown partially And/or The consequence of the attack was explained to some extent.	A FDI attack against the Server (Mosquitto Broker) was shown And The consequence of the attack was shown And The consequence of the attack was explained.
T6 – IDS Alert **(20% - 8 marks)**	The IDS is not configured as required And/or IDS did not generate a suitable alert based on the attack And/or Output is not explained.	The IDS is configured as required And/or IDS alerts based on the attack And/or Output is explained.	The IDS is configured as required And IDS alerts based on the attack And Output is explained.
T7 – MQTT Authentication **(30% - 12 marks)**	MQTT authentication is not configured as required And/or Authentication is not demonstrated successfully	MQTT authentication is configured as required And/or Authentication is demonstrated successfully	MQTT authentication is configured as required And Authentication is demonstrated successfully
T8 – FDI attack repeat **(3% - 1.2 marks)**	A FDI attack against the Server (Mosquitto Broker) was not shown And/or The consequence of the attack was not shown And/or The consequence of the attack was not explained.	A FDI attack against the Server (Mosquitto Broker) was shown partially And/or The consequence of the attack was shown partially And/or The consequence of the attack was explained to some extent.	A FDI attack against the Server (Mosquitto Broker) was shown And The consequence of the attack was shown And The consequence of the attack was explained.
T9 – Additional security control	An additional security control has not been implemented to enhance the current setup AND/OR The control is not demonstrated AND/OR Has been not been justified.	An additional security control has been implemented to enhance the current setup AND/OR The control is demonstrated to some extent AND/OR Has been justified based on the context of the IoT setup.	An additional security control has been implemented to enhance the current setup AND The control is demonstrated to be working as expected AND Has been justified based on the context of the IoT setup.

Note: During marking, you may be given some general comments not related to the marking for improvement in future assignments/studies.