

Team: TEAM 3

Team members: Aidan Curley Ian Wolloff & Kaoru Kitamura

Marker: Dr Cathryn Peoples

Date: April 2022

Criteria	Level	Comments
Knowledge and under-standing of the topic / issues under consideration (25%)	Excellent – Distinction	<p>The system requirements in Table 2 are presented from a limited perspective, and perhaps there is an opportunity here to make it explicit that the perspective is a security one. Otherwise, I might expect to see that the amount of system memory, as one example, would also be included in this list.</p> <p>In relation to the system assumptions, there is an opportunity to describe the users who you are assuming to use the system.</p>
Application of knowledge & understanding (25%)	Excellent – Distinction	<p>In terms of functional requirements in Table 3, security is generally recognised as a non-functional requirement - Methinee Amorndettawin and Twittie Senivongse. 2019. Non-functional Requirement Patterns for Agile Software Development. In Proceedings of the 2019 3rd International Conference on Software and e-Business (ICSEB 2019). Association for Computing Machinery, New York, NY, USA, 66–74. DOI:https://doi.org/10.1145/3374549.3374561. Scalability and fault tolerance are also considered as non-functional requirements.</p> <p>In terms of functional requirements, I would like to see more explicitly the functions that the system will enable. This could include the creation of a user profile, for example, and ability to upload/download a file.</p> <p>I really like how you have considered the proactive security control application from the perspective of OWASP. This demonstrates good alignment between the theory studied and its application in practice.</p> <p>Excellent range of approaches considered to secure the system, including Regex.</p> <p>Great attention to detail consideration of the tests which will be applied, including unit and user acceptance.</p>
Criticality (25%)	Excellent – Distinction	<p>An excellent range of technologies are proposed to be applied in the system deployment, including Snort for intrusion detection and Kafka for queue control.</p>

		<p>On what basis have you reached an assumption that communication will take place using TCP/IP? Have you read any material that supports this assumption?</p>
<p>Structure & Presentation (25%)</p>	<p>Excellent – Distinction</p>	<p>Please note it is convention to number and label figures at the bottom of the diagram.</p> <p>Please re-check your referencing approach. Instead of “(2018, Malesky)”, we would hope to see “(Malesky, 2018)”.</p> <p>Excellent attention given to the presentation & style applied, even down to the font style.</p> <p>Please ensure that all acronyms are defined in full the first time they are used in a document. After that point, the acronym alone may be used.</p> <p>I would like references to be included for all software which you are planning to use in your deployment.</p> <p>Please pay attention to ensuring that capital letters are used, and not used, in the correct places.</p> <p>It is particularly effective that the reference list has been organised according to those which are academic and non-academic.</p> <p>The tables have been presented as figures, and I appreciate the reason why this has been done through our earlier conversation. Just something to keep in mind in relation to this for the future is that a reader may be looking for specific topics in your work to examine if they have been covered. When the text has been included in a figure, this check cannot be made, and important detail may be missed in this way.</p> <p>I really like that this report does not have a massive Appendix, and that mostly the entire report is communicated through the main body contents. This greatly supports readability and understanding of the work.</p>

Overall comments

Positives:

- Excellent attention has been given to harnessing a broad range of technologies to support the design of your system. This is an ambitious programme of work. I am looking forward to seeing, in particular, the application of Snort and Kafka in your software (although I do not see Snort included in Table 7).
- Excellent alignment of proactive security control in your system with industry practices (OWASP).
- Overall, there is excellent attention given to detail in your report, and the diagrams are precisely and professionally defined.

Points for development:

- Please include references for all software mentioned in your report.
- Please check your understanding of functional and non-functional requirements. I have noted that a few of the functional requirements are more like non-functional requirements, and I feel that the functional requirements list which remains is incomplete – it does not capture any of the CRUD capability, for example.

Overall Grade: Excellent – Distinction