

## Tutor's Feedback - Executive Summary and App Presentation

**Grade:** 68% (Merit)

**Graded by:** Dr Oliver Buckley

### Feedback comments:

The code demonstrates a basic understanding of attack tree concepts. It can traverse a tree structure recursively and identify nodes ('action' property).

The `cal_value()` function shows a simple logic for summing values. It might need tweaking if probability-based calculations are required in a future version. The code uses functions for modularity, but some variable names could be more descriptive, remember it's important that your code is clear and makes sense to other developers (or yourself in the future!). There should be extensive comments within the functions to explain their logic step by step – this should explain why you have made the choices that you have, rather than just describing the code does. The code handles JSON input, which is a suitable format for attack tree specifications and the graphviz library is a good choice for attack tree visualisations.

No external libraries other than standard ones (json, graphviz) have been used, which is fine, but if remember that if you use any code snippets from anywhere, they should be cited as well.

The attack trees that you have produced look good and demonstrate the basic functionality and concepts that are required. The comment in the `cal_value` function implies that you were intending to consider impact, but it was not total clear as to how well you had grasped the different assessment models available (e.g. monetary vs. probability). You have covered the monetary inputs but it would be useful to get a clearer idea of how you came to these decisions.

The report provides a thorough overview of the application's purpose, its functionalities, and its significance in enhancing security analysis through visual attack trees. This demonstrates a deep understanding of the project's scope and objectives.

The use of attack trees as a model for analysing potential threats is well-grounded in relevant literature, showcasing the student's ability to integrate academic research into practical applications.

The detailed description of the application's functionalities, including JSON input handling, interactive threat valuation, graphical visualisation, and aggregate threat evaluation, shows that you have understood the core ideas well and have thought about an appropriate solution. There is reasonable evidence of testing, to increase confidence in the code.

The report could benefit from a more detailed discussion on user experience design principles that were considered or applied. This might include ease of use, error handling, or feedback mechanisms to guide the user through the application's functionalities. Exploring potential advanced features or discussing scalability considerations could provide insights into how the application could evolve to meet future needs or handle larger, more complex attack trees.

A deeper critical analysis of the application's limitations or potential areas for improvement would strengthen the report. This might include a discussion on the challenges of accurately valuing threats or the implications of using a simplified model for complex security scenarios.

## **Tutor's Feedback - Individual Reflection**

**Grade:** 80 % (Distinction)

**Graded by:** Dr Oliver Buckley

### **Feedback comments:**

You've taken a deep dive into the knowledge and skills gained from the Information Security Management (ISM) module, guided by the framework proposed by Jones (2021). This approach has allowed you to not only recount the key concepts and principles learned but also to reflect on their application in real-world scenarios. Your goal to achieve a deeper understanding of information security is great and sets a solid foundation for your further development in this field.

Your journey through the ISM module has broadened your perspective on security and risk, encompassing a wide array of topics from risk assessment methods to security standards and disaster recovery solutions. Your previous experience in assisting companies through digital transformations has provided a practical backdrop against which you've measured and enriched your learning. This real-world context has undoubtedly enhanced your comprehension and appreciation of the module's content.

The reflections on your emotional journey through the module, it's clear that it has been both challenging and transformative. The module has provided you with invaluable insights into various aspects of information security management, significantly impacting your professional life and personal development. However, you've also identified the lack of student collaboration and discussion as a drawback.

Since completing the module, you've directly applied your new knowledge to your role, particularly in the adoption of Tenable for vulnerability management and the SOC framework for compliance. This practical application speaks volumes about the

module's relevance and your proactive approach to professional development. Your role as an IT senior engineer requires a nuanced understanding of security measures, something that this module has evidently bolstered.

Your analysis highlights the significance of GDPR compliance and the legal implications of non-compliance, reinforcing the necessity of aligning ISM implementations with GDPR guidelines. This is a critical consideration for your organisation and underscores the importance of a comprehensive approach to information security management.