FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Review report of a final thesis

Reviewer:	Ing. Tomáš Vondra, Ph.D.
Student:	Jakub Šimůnek
Thesis title:	Architektura a technologie bezpečnostního dohledového centra (SOC)
Branch / specialization:	Computer Security and Information technology
Created on:	21 January 2024

Evaluation criteria

1. Fulfillment of the assignment

▸ [1] **assignment fulfilled**
[2] assignment fulfilled with minor objections
[3] assignment fulfilled with major objections
[4] assignment not fulfilled

No objections.

2. Main written part

70 / 100 (C)

The thesis is very nicely structured and written without any typos and factual mistakes. From typographic perspective I have an objection to the too small size of the text in figures. The theoretical part summarizes the objective and roles within an SOC team and the technologies they use. There are a lot of chapters that lack a citation or only cite a marginal fact (see 1.5.1). To be clear, I do not want to say that there is any plagiarism involved. These paragraphs contain well-known facts. But from the amount of them we can judge that the content brings little added value to the informed reader. This corresponds to the quality of references which are exclusively articles from popular Internet magazines or security solution vendors.

3. Non-written part, attachments

80 / 100 (B)

There are no actual attachments, but the practical part of the thesis describes the building of a lab setup that simulated a network and its security monitoring infrastructure, all using open-source. The setup looks good. The only thing I would like to see more elaborated is the choice of components. The text talks about "careful consideration", but doesn't really list the properties of the considered components. Some problems with compatibility are then found with the chosen SIEM solution "Wazuh". Could

they be expected with other open-source solutions as well? Also, the quality of detection rules in the system was not evaluated against commercial solutions.

4. Evaluation of results, publication outputs and awards 80 /100 (B)

The setup described in the thesis can be deployed in practice to monitor a home network or a garage-sized tech company.

The overall evaluation 80 /100 (B)

Overall, I find that the main focus of the thesis was to build a security monitoring solution that is cheap and applicable at a small scale, which was a success. I would have appreciated more focus on the description of the choice of components than the general information which is in the theortical part.

Questions for the defense

What changes to the logging solutions would be necesary in order to monitor a home network based predominantly on Cisco devices?

Instructions

Fulfillment of the assignment

Assess whether the submitted FT defines the objectives sufficiently and in line with the assignment; whether the objectives are formulated correctly and fulfilled sufficiently. In the comment, specify the points of the assignment that have not been met, assess the severity, impact, and, if appropriate, also the cause of the deficiencies. If the assignment differs substantially from the standards for the FT or if the student has developed the FT beyond the assignment, describe the way it got reflected on the quality of the assignment's fulfilment and the way it affected your final evaluation.

Main written part

Evaluate whether the extent of the FT is adequate to its content and scope: are all the parts of the FT contentful and necessary? Next, consider whether the submitted FT is actually correct – are there factual errors or inaccuracies?

Evaluate the logical structure of the FT, the thematic flow between chapters and whether the text is comprehensible to the reader. Assess whether the formal notations in the FT are used correctly. Assess the typographic and language aspects of the FT, follow the Dean's Directive No. 52/2021, Art. 3.

Evaluate whether the relevant sources are properly used, quoted and cited. Verify that all quotes are properly distinguished from the results achieved in the FT, thus, that the citation ethics has not been violated and that the citations are complete and in accordance with citation practices and standards. Finally, evaluate whether the software and other copyrighted works have been used in accordance with their license terms.

Non-written part, attachments

Depending on the nature of the FT, comment on the non-written part of the thesis. For example: SW work – the overall quality of the program. Is the technology used (from the development to deployment) suitable and adequate? HW – functional sample. Evaluate the technology and tools used. Research and experimental work – repeatability of the experiment.

Evaluation of results, publication outputs and awards

Depending on the nature of the thesis, estimate whether the thesis results could be deployed in practice; alternatively, evaluate whether the results of the FT extend the already published/known results or whether they bring in completely new findings.

The overall evaluation

Summarize which of the aspects of the FT affected your grading process the most. The overall grade does not need to be an arithmetic mean (or other value) calculated from the evaluation in the previous criteria. Generally, a well-fulfilled assignment is assessed by grade A.