Title: "An Investigation of Log Data Analysis for IT Security Threat Detection"

# Abstract

The increasing dependence on technology in today's world has made IT security a critical concern. To protect against security threats (like/such as …[[1]](#footnote-1)), organizations need to have robust security measures (like/such as …[[2]](#footnote-2)) in place, which includes monitoring and analysing log data. The purpose of this thesis is to investigate the use of log data analysis for IT security threat detection. The thesis will explore various techniques (like/such as …[[3]](#footnote-3)) for analysing log data to identify patterns and anomalies that indicate potential security threats. In addition, the thesis will involve several micro-projects to demonstrate how log data analysis can be used to detect specific security threats such as unauthorized access attempts[[4]](#footnote-4), malware infections[[5]](#footnote-5), and phishing attacks[[6]](#footnote-6). The projects will involve collecting log data from various sources such as firewalls, intrusion detection systems, and web servers, key-logs[[7]](#footnote-7), etc. and applying different analysis techniques[[8]](#footnote-8) to identify potential security threats. The results of the projects will be evaluated to determine the effectiveness[[9]](#footnote-9) of log data analysis for IT security threat detection. This thesis aims to provide insight into the role[[10]](#footnote-10) of log data analysis in IT security and to demonstrate its practical applications[[11]](#footnote-11) through micro-projects.

Please: complete the expected lists (see footnotes below) based on chatGPT in form of annexes of this document!

# Annexes

## List#1: …

## List#i: …

## List#n: …

1. This list about security threats should be completed e.g., based on chatGPT… [↑](#footnote-ref-1)
2. This list about security measures should be completed e.g., based on chatGPT… If the list is completed, the elements of the list should be evaluated at least in 3 subgroups: robust – non-robust – I-do-not-know/depending-on… [↑](#footnote-ref-2)
3. This list about various techniques should be completed e.g., based on chatGPT… [↑](#footnote-ref-3)
4. <https://miau.my-x.hu/mediawiki/index.php/System-modeling#Automation_of_Incident_Response_Planning_in_IT_Security_.28AIR-P-ITS.29> 🡨this can be seen as a micro-project! [↑](#footnote-ref-4)
5. <https://miau.my-x.hu/mediawiki/index.php/System-modeling#Antivirus_project> 🡨this will be a micro-project ASAP… [↑](#footnote-ref-5)
6. <https://miau.my-x.hu/mediawiki/index.php/System-modeling#Expert_system_for_fine-tuning_IT-security_systems_.28ES-FITS.29> 🡨this can be seen as a micro-project! [↑](#footnote-ref-6)
7. <https://miau.my-x.hu/miau2009/index.php3?x=e0&string=2dm> 🡨demo for a big project… [↑](#footnote-ref-7)
8. This list about analysis techniques should be completed e.g., based on chatGPT… [↑](#footnote-ref-8)
9. Effectiveness and efficiency should be defined immediately for each micro-project and parallel, information added-values should also be derived for each system-modelling-project before closing a micro-project! [↑](#footnote-ref-9)
10. This list about potential roles should be completed e.g., based on chatGPT… [↑](#footnote-ref-10)
11. (((Each thesis will need an application (source codes) too - by the end of the BPROF-education!))) [↑](#footnote-ref-11)