Introduction

On a Friday morning, Swiss National Cyber Security Centre (NCSC) receives a report about a critical vulnerability in a popular Java library called Log4j. At the time of receiving these reports, the vulnerability apparently is exploited by threat actors “in the wild” and no patch is available to fix the vulnerability (0-day exploit).

You are security analyst in a large company’s Security Operation Center (SOC) and soon as you got the security advisory forwarded, you receive already questions about the new vulnerability from concerned colleagues. The operation manager scheduled a meeting to discuss the situation for the company and action needs. You will be asked to present an overview about the vulnerability and the threat to the company. Goal and Tasks

To be prepared for the meeting, perform an analysis of the given security advisory and work out the following five topics in a written report:

- Sketch a pictural overview how the log4j attack works (so that you would be able to present an attack overview on a flipchart in the meeting).
- Give a description of the problem(s) of the log4j attack, why is it rated critical.
- Relevance: Describe why this attack is relevant for any company.
- Challenges: Describe three different challenges that make it difficult to solve the problem.
- Next steps: Describe three different organizational or technical steps to tackle the problem.

Submission

Submit a written report as a PDF document, containing the information structured as outlined in the goal and tasks section