To systematically assess potential threats to our system, we applied the STRIDE threat modelling framework. This revealed high-impact vulnerabilities around authentication, LLM output handling, and API abuse. We implemented mitigations such as OAuth2 token validation, input/output sanitisation, and rate limiting. These measures reduce our system’s exposure to spoofing, tampering, and denial-of-service attacks, while aligning with industry best practices in secure software development. (Kloda, 2025)

# References

Kloda (2025). [online] github. Available at: https://github.com/Jkloda/LOJuliaKloda/blob/main/LongTailOfTheSoftwareCycle/STRIDE.xlsx [Accessed 21 May 2025].