# Threat Model (Light)

## Service Desk AI Knowledge Tool

Date Assessed: May 2025

Prepared by: Trefor Walters

Reviewed by: Will North

### Background

The Service Desk AI (SDAI) Knowledge Tool is an AI-powered knowledge base system. The bulk of the components responsible exist in Azure, but as a proof-of-concept to quickly prototype and work with these components, a user interface has been created in Excel, underpinned with code written in Visual Basic for Applications. The system is designed to process existing support cases where a known solution was found, redact any sensitive information, process the remaining data via an LLM, and retrieve them in the form of knowledge articles to support customers. The design allows for both the creation of new knowledge articles and the management of existing ones, with the Excel interface serving as a quick way to demonstrate the feasibility of the underlying Azure-based architecture before committing to full frontend application development.

### Scope

This threat model assesses what threats might be introduced by the SDAI tool and seeks to understand the extent of any mitigations. The scope is limited to the Excel and VBA elements only, with the cloud and LLM components out of scope as they are not specific to this tool.

### Threat Assessment

The following key threats were identified and assessed.

|  |  |  |
| --- | --- | --- |
| **Threat** | **Mitigation** | **Mitigated** |
| **High:** Hardcoded API keys and URLs could be stolen from the Excel document and misused. | Access is limited to the Excel file to a small number of authorised personnel only and the VBA project is password protected inside the document. | **Yes** |
| **Medium:** A threat actor could submit malicious data to the API end points via the Excel document. | The cells used to submit data to the API are sanitized and / or are range bound. | **Yes** |
| **Medium:** Customer data may be ingested into the LLM and used in generative content. | Sanitisation is undertaken on the data that is consumed so that it is not sent to the AI model. Manual checks are also undertaken on the generated knowledge article content to ensure personal data is not included. | **Yes** |

### Conclusion

The design should proceed to implementation as all key threats are sufficiently mitigated.