**Protokoll – 1. Workshop: Expertenrunde zum KI-gestützten Threat Modelling**

**Datum:** ??.05.2025  
**Ort:** Universität Bremen, MZH, Raum 6300  
**Dauer:** 10:00 – 12:00 Uhr  
**Teilnehmer:** LLM-Experten, Security-Experten, Software Engineering-Experten (je 2 Personen)  
**Ziel des Workshops:**

* Diskussion und Feedback zu Konzept, Methode und Tools der geplanten Studie
* Identifikation von Herausforderungen, Gaps und Chancen
* Audioaufnahme zur späteren Auswertung

**Zeitplan**

**09:30 – 09:40** – Begrüßung & Vorstellung der Teilnehmenden  
**09:40 – 10:20** – **Präsentation der Studienidee**

* Motivation, Zielsetzung, Forschungsfragen
* Konzept des Tools
* Kurze Darstellung bestehender Studien & Erkenntnisse

**10:20 – 10:30** – Beispiel-Demonstration

**10:30 – 12:00** – **Diskussion & Experteninterview (Audioaufnahme)**

**Diskussionsleitfaden / Fragen:**

Konzept validieren Ist das Vorgehen sinnvoll?

1. Ist das Vorgehen sinnvoll? Was fehlt?
2. Wo sind Herausforderungen aus Sicht von LLM / Security / Software Engineering?
3. Welche Verbesserungen oder Alternativansätze schlagen Sie vor?
4. Welche Tools sind geeignet – warum?
5. Wann ist menschlicher Input notwendig? Wo explizit?
6. Welche Prompt-Typen führen zu brauchbarem Output?
7. Unterschiede zwischen textueller Prompt-Eingabe vs. grafischer (DFD als Bild)?
8. Chain-of-Thought nutzbar? Wie könnte das aussehen?
9. Wie kann man Vertrauen in ein KI-basiertes System schaffen?
10. Welche Visualisierungen oder Formate wären hilfreich für die Kommunikation mit dem Tool (z. B. Text, DFD, Flowcharts, Tabellen)?

Domänenübergreifende Perspektiven abbilden

1. Welche Informationen fehlen Ihnen aktuell noch, um sich ein vollständiges Bild vom geplanten Prozess zu machen?

LLM-Experten

Welche Sinschränkunegn bei Anwendung LLMs auf DFDs

Welche Arten von Pormpts, Eingabeformaten sind gut

Wie Entschieudngfindenung bei Personen ohne ML Hintergrund versäntlich erklären

Sicherheit-Experten

Typische Schmerzpunkte beim STRIDE-basieren Threat Modelling mit DFDs

Wichtige Erklärbarkeit

Mindesr