AI Threat Modeling MCP Server - FREE SAMPLE

AI-Powered Threat Modeling MCP Server: Build It From Scratch

A Complete Guide to Building an MCP Server for Structured STRIDE Threat Analysis

---

Author: Joseph Thachil George

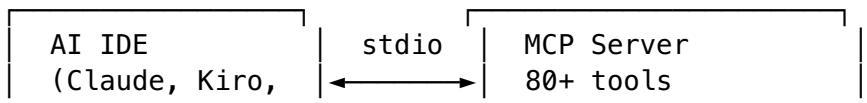
What You Get in the Full Book

- **60 pages** of hands-on, code-driven content
- **24 chapters** covering every module from scratch
- Complete source code with line-by-line explanations
- 5 real-world use cases with working examples
- Docker deployment guide
- AI assistant configuration for Claude, Kiro, Cursor, Copilot
- Full 80+ MCP tools reference table

About This Project

The **AI-Powered Threat Modeling MCP Server** is a Model Context Protocol (MCP) server that gives AI coding assistants structured threat modeling capabilities. Instead of asking an AI to "do a threat model" and receiving unstructured prose, this server provides **80+ specialized tools** that guide the AI through a rigorous 9-phase STRIDE methodology.

How It Works



1. Configure your AI IDE to connect to this MCP server
2. Your AI assistant gains access to 80+ threat modeling tools
3. Describe your system in natural language
4. The AI conducts a structured 9-phase STRIDE analysis
5. Export a complete threat model in JSON format

The 9-Phase Workflow

Phase	Name	Key Tools
1	Business Context	`set_business_context`, `get_organization_guidelines`
2	Architecture	`add_component`, `add_connection`, `add_data_store`
3	Threat Actors	`add_threat_actor`, `analyze_threat_actors`
4	Trust Boundaries	`add_trust_zone`, `add_crossing_point`
5	Asset & Data Flows	`add_asset`, `add_flow`
6	Threat Identification	`add_threat` (STRIDE-based)
7	Mitigation Planning	`add_mitigation`, `link_mitigation_to_threat`
8	Residual Risk	`validate_against_guidelines`
9	Export	`export_threat_model` (JSON)

Key Features

- **80+ MCP tools** organized by threat modeling domain
- **Customizable guidelines** — edit `.md` files, no code changes
- **Case-insensitive enum validation** — graceful AI interactions
- **JSON export** — AWS Threat Composer compatible
- **Docker support** — deploy for teams via SSE transport
- **Works with any MCP AI** — Claude, Kiro, Cursor, Copilot

Technology Stack

Technology	Purpose
Python 3.10+	Runtime
FastMCP	MCP server framework
Pydantic v2	Data validation
Loguru	Structured logging

Technology	Purpose
Docker	Container deployment

What's Inside the Full Book

Chapters	Topic
1–3	MCP protocol, STRIDE methodology, architecture overview
4–7	Setup, data models, enum validator, server entry point
8–16	All 11 tool modules built from scratch with full code
17–19	Utilities, Docker deployment, AI assistant configuration
20–21	Full threat model session walkthrough, guideline customization
22–24	Testing, CI/CD, extending the server, conclusion
Appendices	File listing, 72-tool reference table, environment variables
Source Code	Full repository on GitHub

Get the full book to build this MCP server from scratch.

Source code: **https://github.com/aisecuritytools-ai/ai-powered-threat-modeling-mcp-server**

> *This is a FREE SAMPLE. The full book contains 60 pages with complete source code, detailed explanations, and step-by-step build instructions.*