

# STRIDE GPT

Revolutionising Threat Modelling with GenAI

Matt Adams

26<sup>th</sup> February 2025



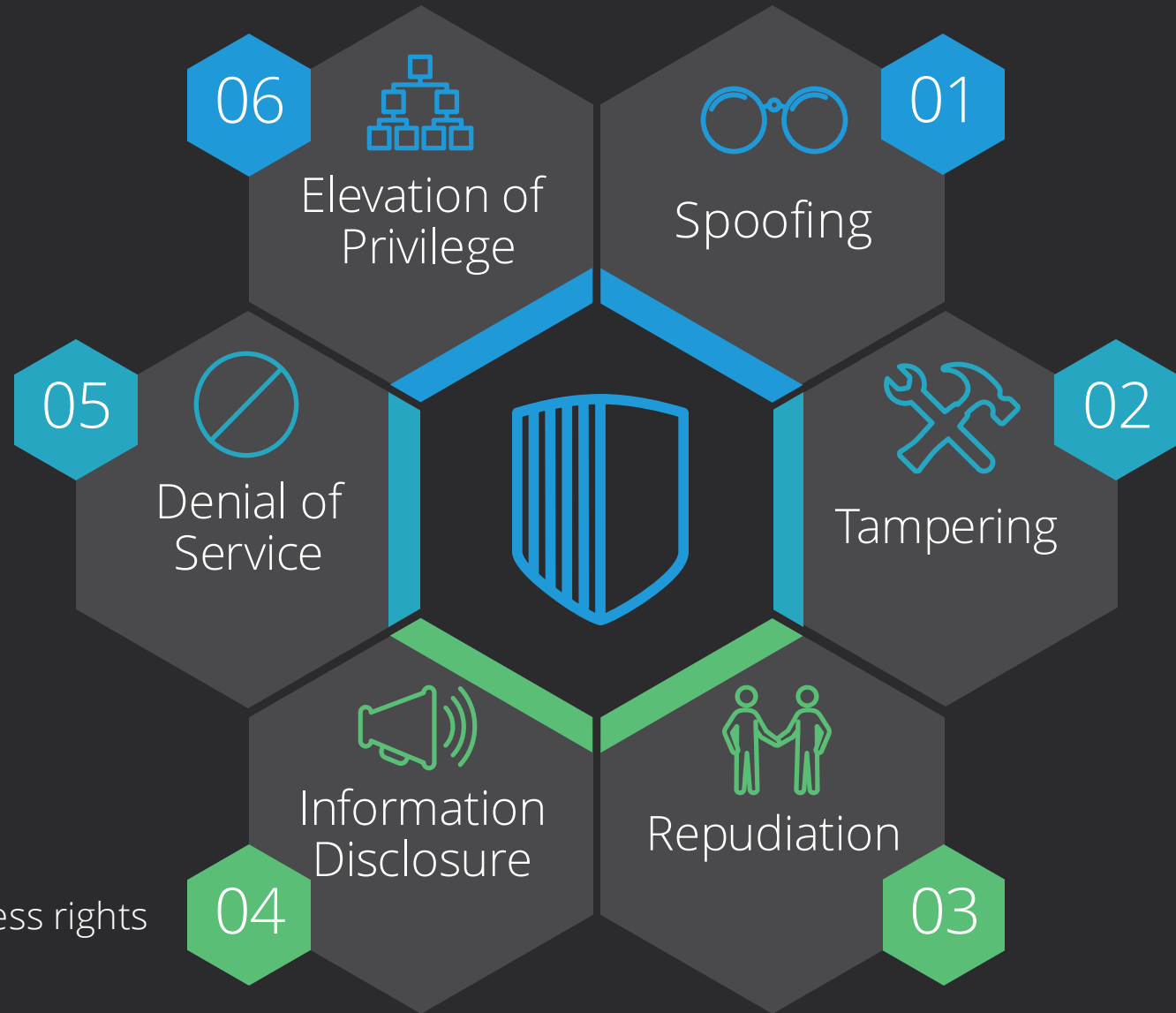
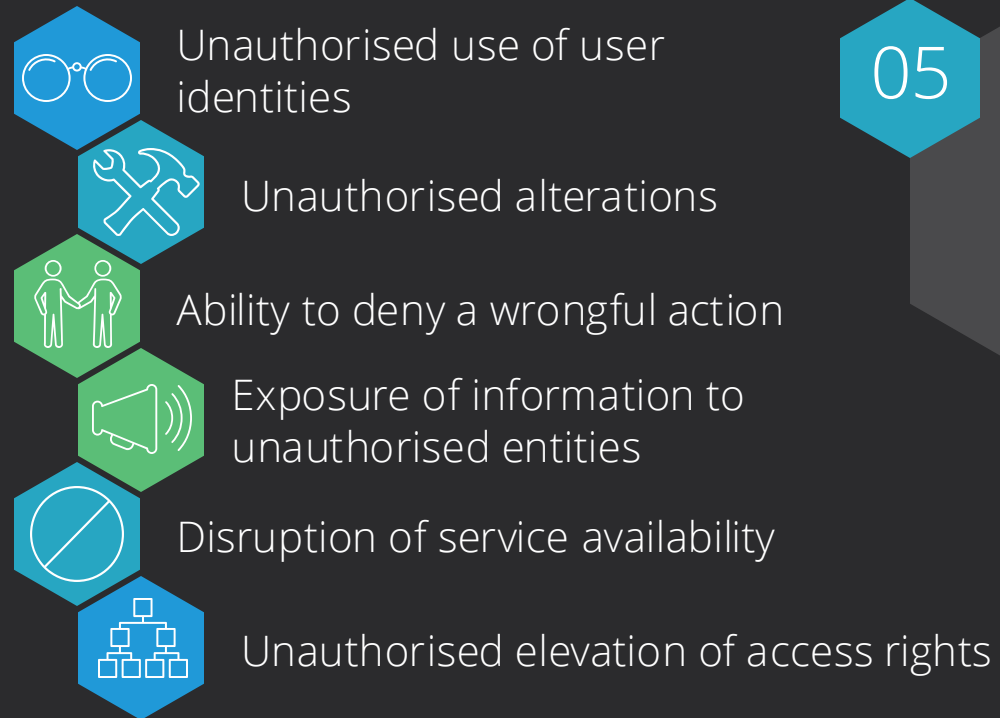
# Agenda

- |   |                            |   |                   |
|---|----------------------------|---|-------------------|
| 1 | Introduction               | 5 | Live Demo         |
| 2 | STRIDE Methodology         | 6 | Adoption & Impact |
| 3 | Introduction to STRIDE GPT | 7 | Future Plans      |
| 4 | Key Features and Updates   | 8 | Q&A               |

# Introduction

# STRIDE

An overview of the methodology





# STRIDE GPT

## Concept



- **Empowering Non-Security Experts:** Designed to assist those without security expertise in generating realistic initial threat models.
- **Efficient Use of Resources:** Frees up scarce security resources from basic modelling, enabling focus on complex analysis and refinement.
- **Facilitating Collaborative Security:** Provides a solid baseline for non-security personnel, fostering a more security-aware culture.
- **Iterative Refinement:** The tool's output serves as a starting point for further detailed and nuanced threat modelling.

# STRIDE GPT

## Key Features & Recent Updates

### Key Features

- Multi-modal threat modelling
- Attack Trees
- Threat mitigation suggestions
- DREAD risk assessments
- Gherkin test cases

### Updates

- Generate outputs using latest reasoning models (o1, o3-mini, DeepSeek R1)
- Support for local LLMs using either Ollama or LM Studio
- Use a GitHub repo as an input to a threat model
- Improved Attack Tree diagram generation
- Enhanced JSON output handling across all model providers



# Demos


1

Threat Model

2

Repo Analysis

# Demo 1: Threat Model Generation



**STRIDE GPT**

How to use STRIDE GPT

Select your preferred model provider:

OpenAI API

1. Enter your [OpenAI API key](#) and chosen model below
2. Provide details of the application that you would like to threat model
3. Generate a threat list, attack tree and/or

Threat Model | Attack Tree | Mitigations | DREAD | Test Cases

A threat model helps identify and evaluate potential security threats to applications / systems. It provides a systematic approach to understanding possible vulnerabilities and attack vectors. Use this tab to generate a threat model using the STRIDE methodology.

Enter GitHub repository URL (optional)

<https://github.com/owen1e/vego>

Select the application type

Web application

Describe the application to be modelled

Enter your application details...

What is the highest sensitivity level of the data processed by the application?

Top Secret

Is the application internet-facing?

Yes

What authentication methods are supported by the application?

Choose an option

Deploy

## STRIDE GPT v0.12

### Threat Modeling Demo

<https://youtu.be/aaH9nBeKC2A>



# Demo 2: GitHub Repo Analysis



The image shows the STRIDE GPT v0.12 web interface for GitHub Repo Analysis. On the left, there's a sidebar with the STRIDE GPT logo and instructions on how to use the tool. The main area displays the 'Threat Model' tab, which includes a description of threat modeling and a form to generate a threat model. The form has several input fields and dropdown menus for configuring the analysis.

**STRIDE GPT v0.12**  
GitHub Repo Analysis

**How to use STRIDE GPT**

Select your preferred model provider:

Graql API

1. Enter your [Graql API key](#) and choose model below.
2. Provide details of the application that you would like to threat model.
3. Generate a threat list, attack tree and/or

**Threat Model** | Attack Tree | Mitigations | DREAD | Test Cases

A threat model helps identify and evaluate potential security threats to applications / systems. It provides a systematic approach to understanding possible vulnerabilities and attack vectors. Use this tab to generate a threat model using the STRIDE methodology.

Enter GitHub repository URL (optional)

<https://github.com/owens/repo>

Select the application type

Web application

Describe the application to be modelled

Enter your application details...

What is the highest sensitivity level of the data processed by the application?

Top Secret

Is the application internet-facing?

Yes

What authentication methods are supported by the application?

Choose an option

<https://youtu.be/GhfbEtvdy0>

# STRIDE GPT

## Adoption & Impact

"The idea of saving time on research and threat intel when building an attack tree or a threat model sounds great."

"Really cool and a very good example of the power of Gen AI in AppSec."

"This is incredibly cool Matthew. Time to throw away the spreadsheets! Great work."

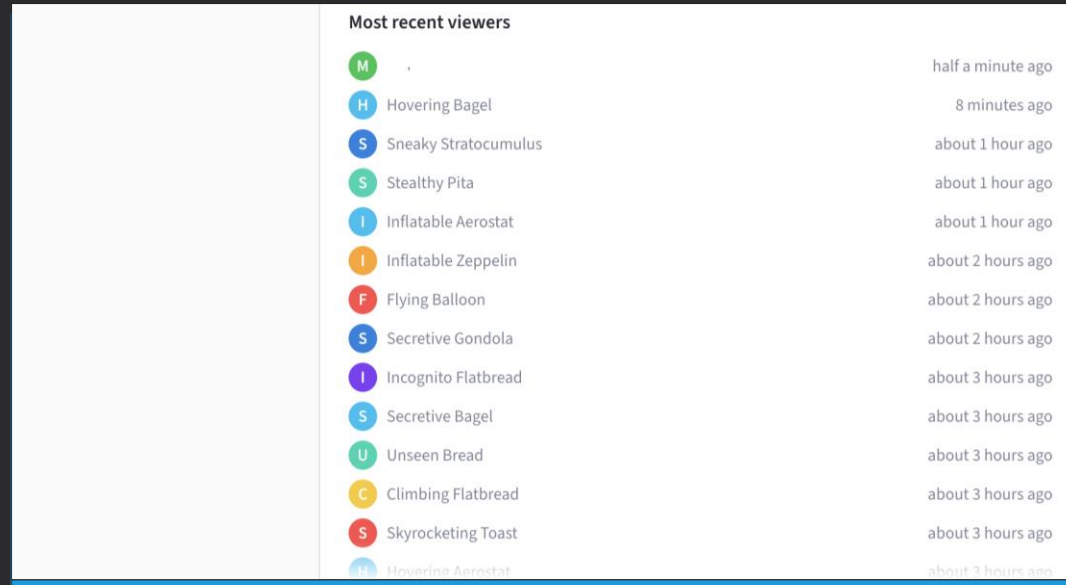
"I'm using it using Azure OpenAI Service. It works great! "

"This is  
🔥 🔥 🔥 🔥 "



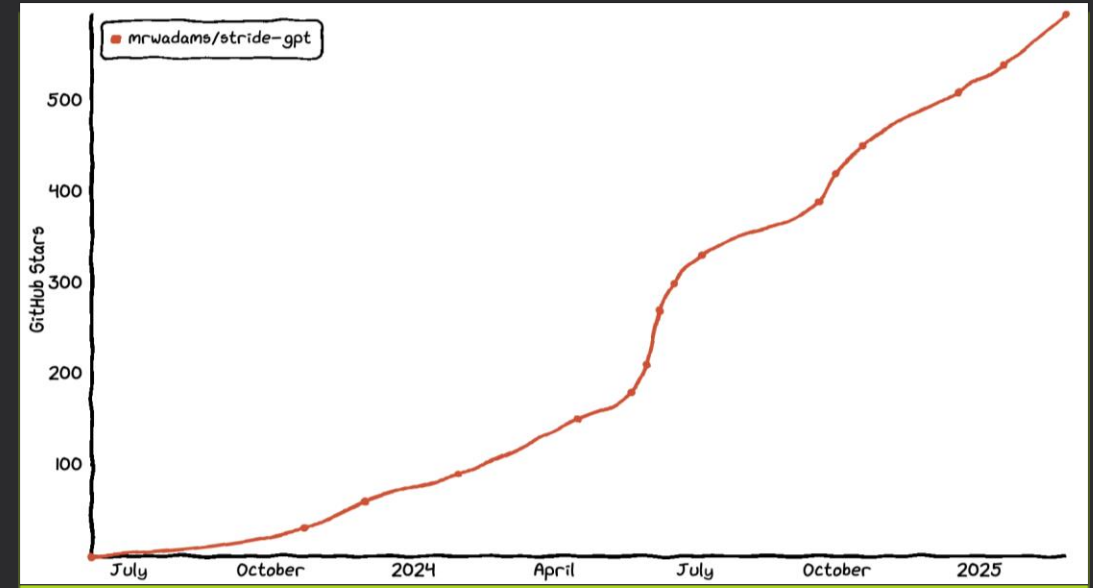
# STRIDE GPT

## Adoption & Impact



### Streamlit Community Cloud

- 18,000+ unique users
- Multiple new users every hour

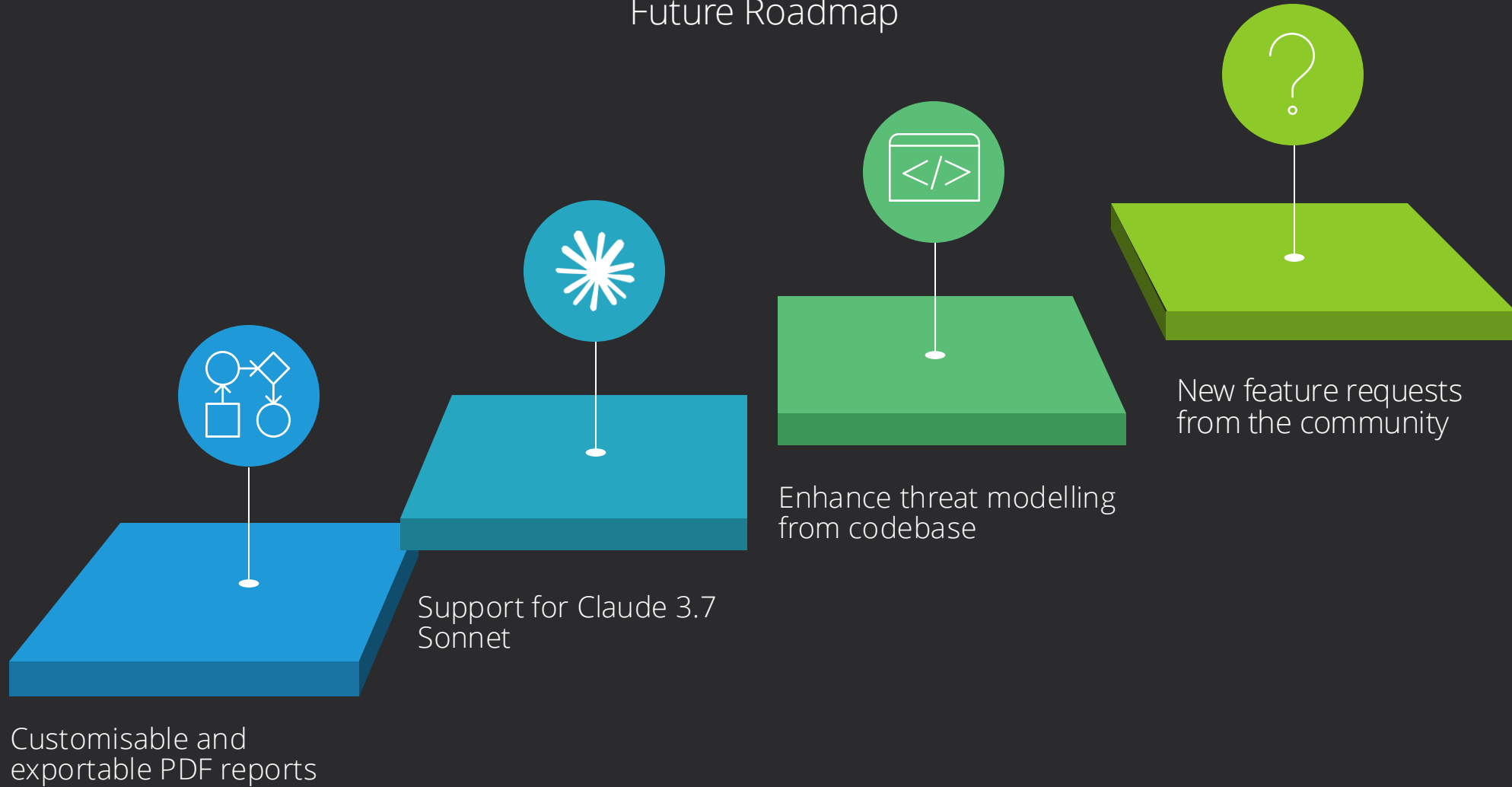


### GitHub Repo

- 594 stars
- 182 forks

# STRIDE GPT

## Future Roadmap



Q&A





# Thanks!

## GitHub Repo

Please add a ★ if you like the project



<https://github.com/mrwadams/stride-gpt>

## Streamlit App

Quickly test STRIDE GPT

(OpenAI / Azure OpenAI Service / Google / Mistral API key required)



<https://stridegpt.streamlit.app>

<https://www.linkedin.com/in/matthewrwadams/>