



DOING MORE WITH LESS

Practical applications for
generative AI in cybersecurity

Matt Adams



AGENDA

1

INTRO / OBJECTIVES

2

**USE CASE 1:
THREAT MODELLING**

3

**USE CASE 2:
SECURITY
AWARENESS**

4

**USE CASE 3:
WEB APP SCANNING**

5

**IDENTIFYING USE
CASES**

6

BEST PRACTICES

7

Q&A

INTRODUCTION



WORK

Security Architect,
Santander UK



CAREER


Consultant,
Contractor,
Permanent



HOBBIES

Smallholding,
Homelabbing,
Coding

OBJECTIVES

- 
- Demo some tools
 - Raise awareness of practical applications for generative AI in cybersecurity
 - ~~Introduction to generative AI~~
 - ~~Security risks associated with LLMs~~
 - ~~'Chat with documents' use cases~~

USE CASE **1**

Threat modelling with STRIDE GPT

KEY FEATURES

- Prompt templates parameterised with app details
- OpenAI model called with formatted prompt
- Model outputs JSON objects that are parsed into Python dicts

<https://stridegpt.streamlit.app>

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

USE CASE **2**

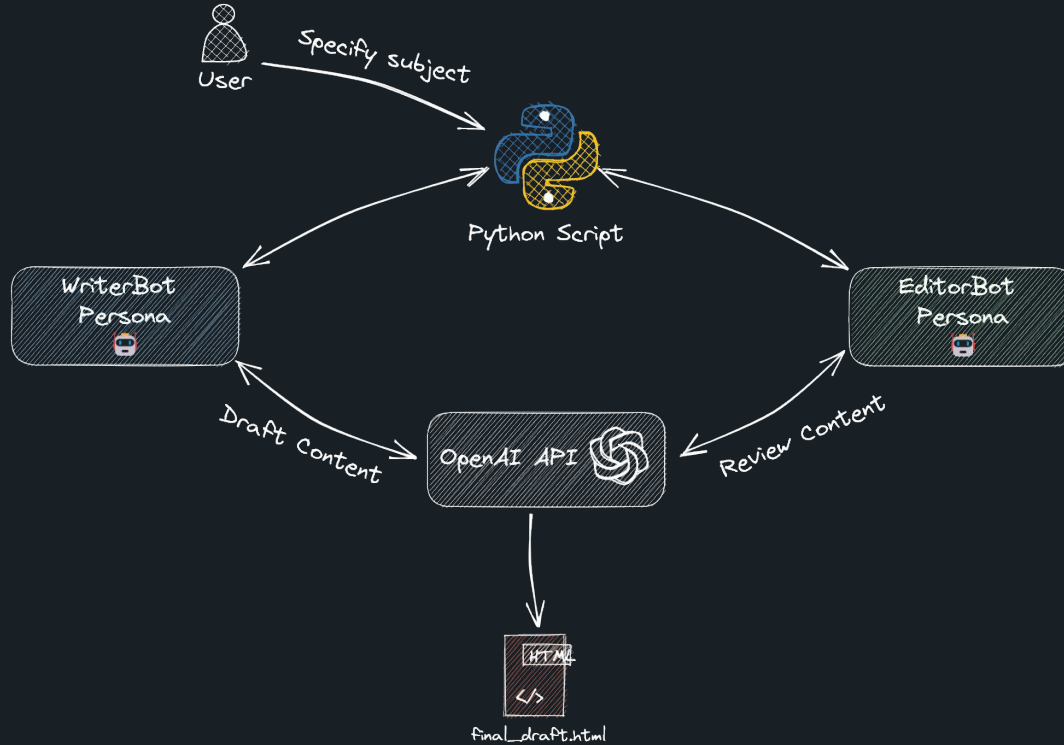
Generating security awareness content using multiple personas

KEY FEATURES

- Simulated conversation between two AI personas
- Use of personas enables specialisation and improves task focus
- Easily customisable to different content generation tasks
 - Add personas, change roles
 - Modify prompts and goals

<https://github.com/mrwadams/beeblebots>


PROCESS FLOW



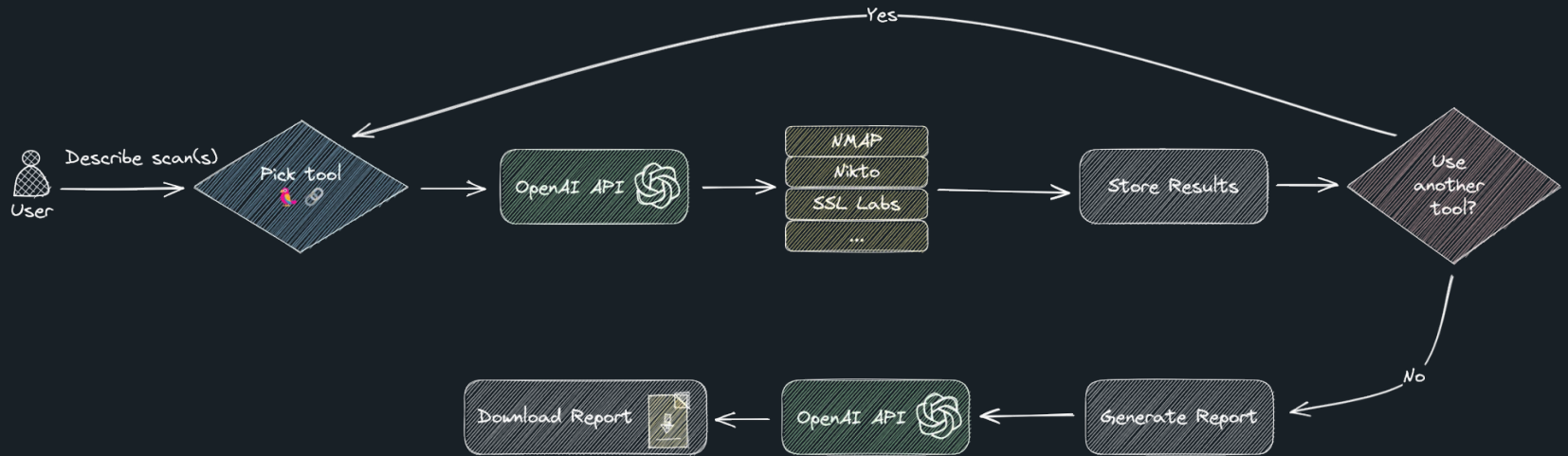
USE CASE **3**

Security scanning and reporting using autonomous agents


KEY FEATURES

- 
- User describes required scan(s) in natural language
 - Agent-based orchestration
 - Agent decides which tool(s) to use based on user request
 - Visibility into agent's "thoughts" to improve transparency


PROCESS FLOW




IDENTIFYING USE CASES

- 
- Imagine you had a new intern - what would you delegate?
 - Good candidates for generative AI are repetitive and/or tedious tasks that can be automated
 - Look for opportunities to augment human capabilities with AI
 - Start small with a well-defined initial use case

BEST PRACTICES

- 
- Start with non-critical use cases
 - Integrate 'human-in-the-loop' reviews
 - Monitor closely for bias
 - Document processes and track performance
 - Be transparent about use of AI

BEST PRACTICES (cont.)

- 
- Evaluate cybersecurity impact
 - Watch out for misplaced over-reliance
 - Keep developing internal AI expertise

Q&A



**ANY
QUESTIONS?**



THANKS!

linkedin.com/in/matthewrwadams
github.com/mrwadams

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**