# Ashurst

AI and Its Integration Problem

My journey to make it work

Euan McGregor
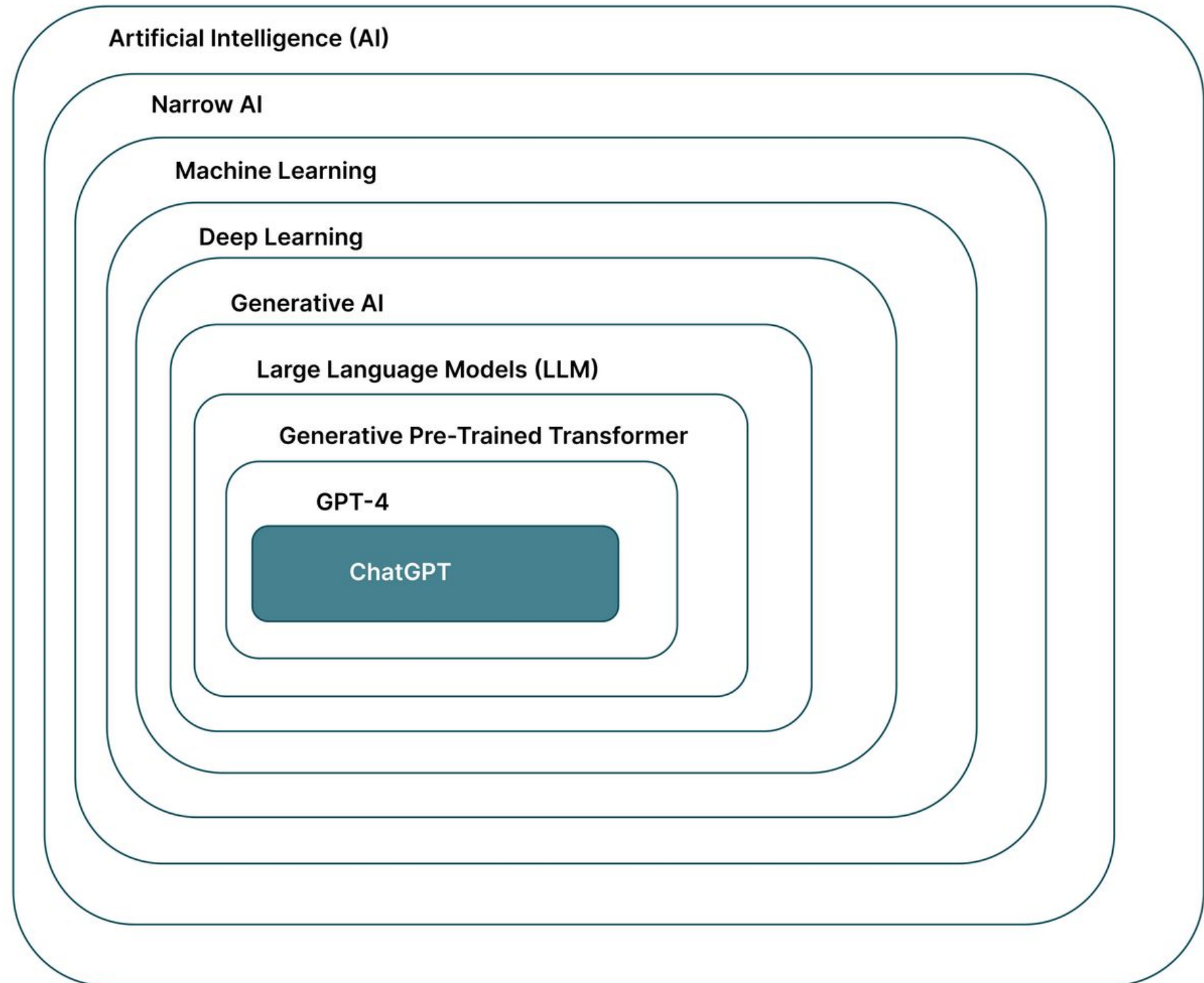Senior Manager, Cyber Security
Ashurst LLP

- My own views and not the views or opinions of my employer.
- Do not share confidential information with an AI.
- AI can be useful and powerful but ensure you follow your organisation policies when utilising AI within your organisation.
- Everything discussed today does not utilise any corporate information and is all publicly available information.
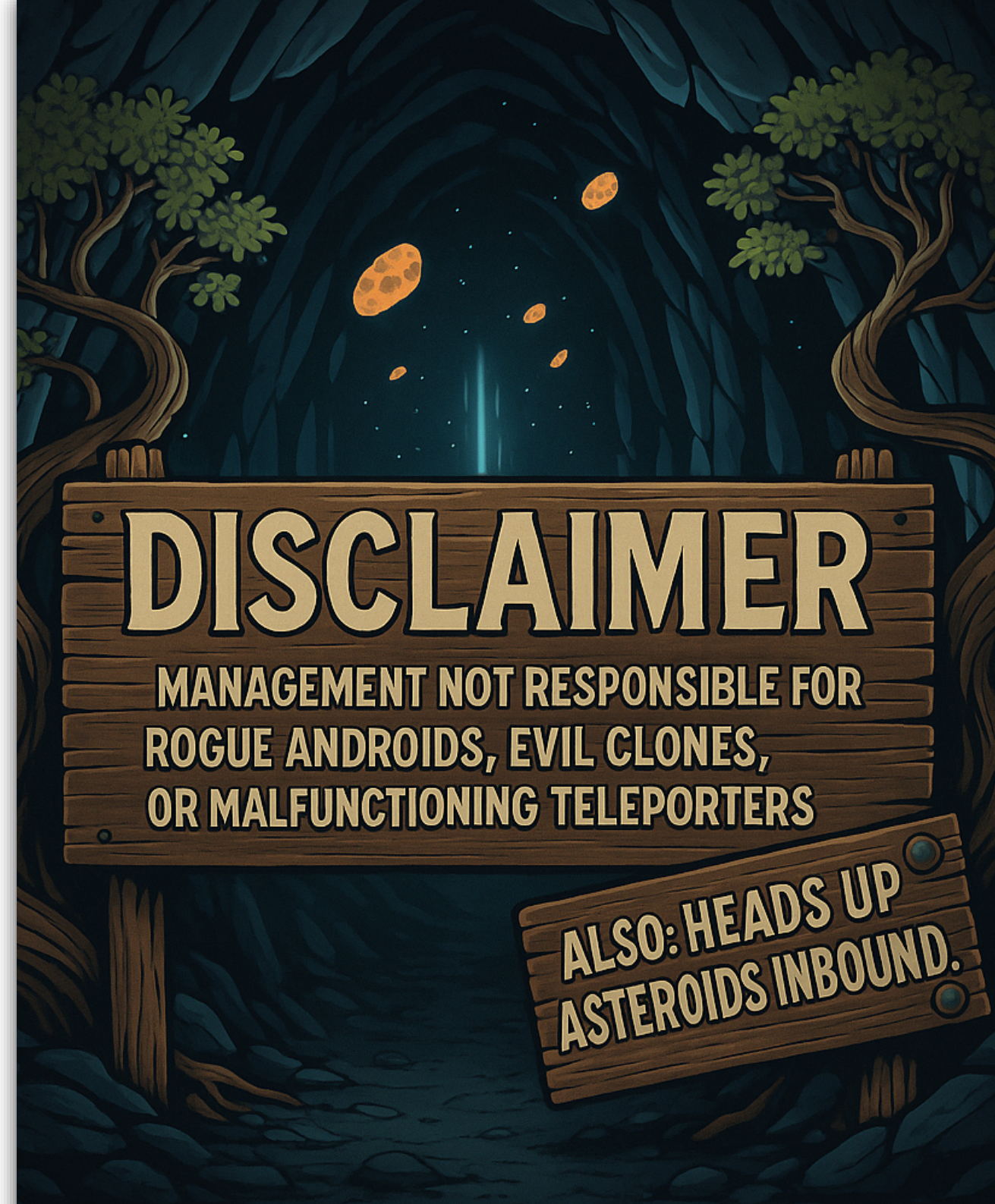
Objectives

- Shifting perspectives on chatbots.

- Create ideas to enhance your daily routine.

- Discover AI features that align with your needs and activities.

- Simplify the process of beginning integration.

Artificial Intelligence Taxonomy

Artificial Intelligence (AI)

Narrow AI

Machine Learning

Deep Learning

Generative AI

Large Language Models (LLM)

Generative Pre-Trained Transformer

GPT-4

ChatGPT

AI in a Nutshell: A Practical Guide to Key Terminology
(https://blog.tobiaszwingmann.com/p/demystifying-ai-
practical-guide-key-terminology)

"It's a mathematical abstraction of the brain...and it's got knobs in it. Many knobs."

Andrej Karpathy

Prominent computer scientist in deep learning and computer vision

Current AI Landscape

- Thousands of AI Tools

- Disconnected Solutions

- The Integration Gap

- Chat Interfaces

- New State of the Art model nearly every week

- Closed Source

- Open Source

Current AI Landscape – Cyber Security

- Integrations within existing products

- AI driven security solutions

- New Features Powered by AI

- Can provide useful insights and help alert fatigue etc.

- Machine Learning over Generative AI
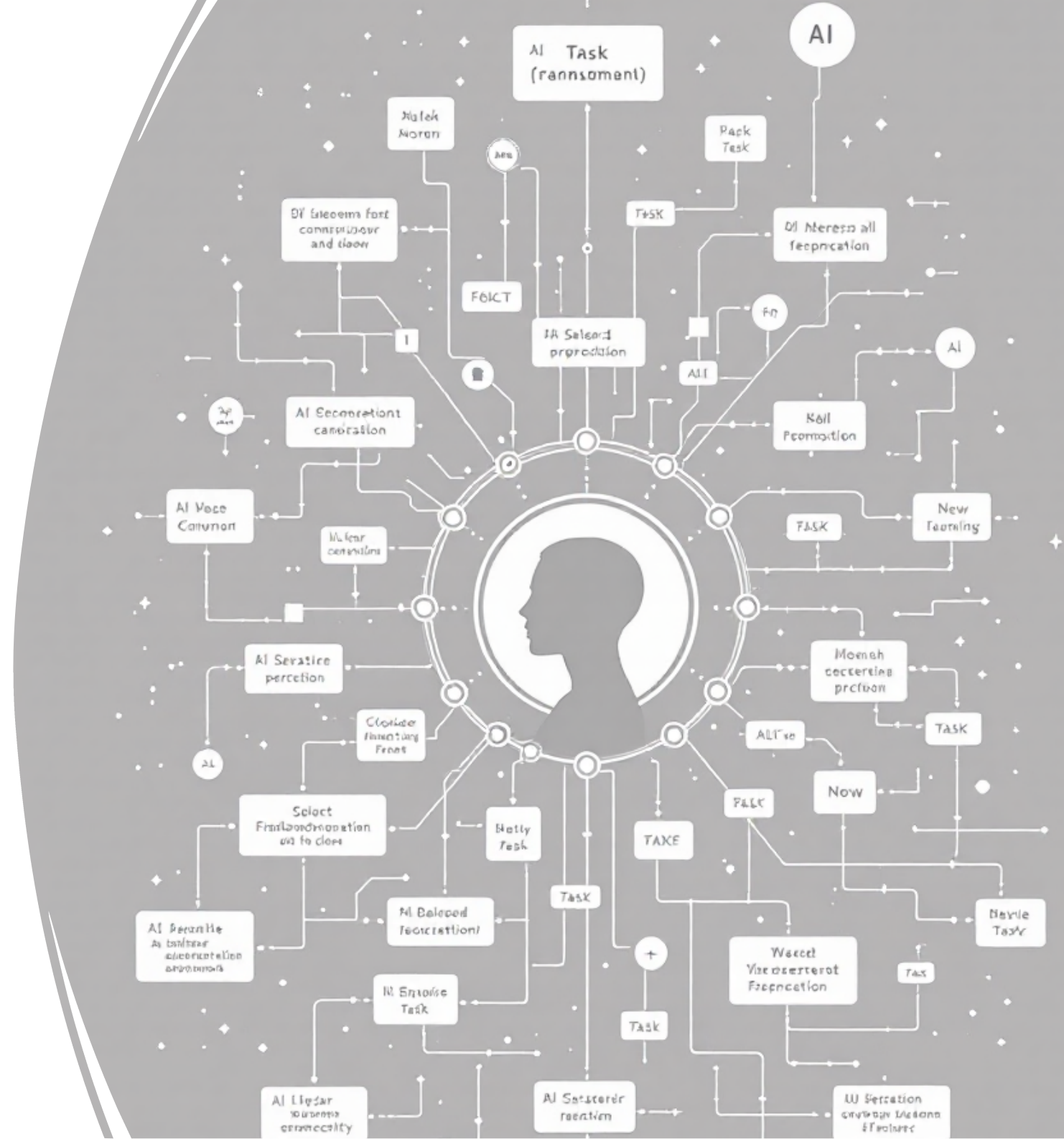
Personal AI - Make it yours

- Custom workflows

- Tailored to you work and personal

- My journey to making AI work for me

- Lower the bar to entry

Prompting and Context

- The LLM is not a mind reader.

- You need to prompt it.

- Tell it what you want from your session with it.
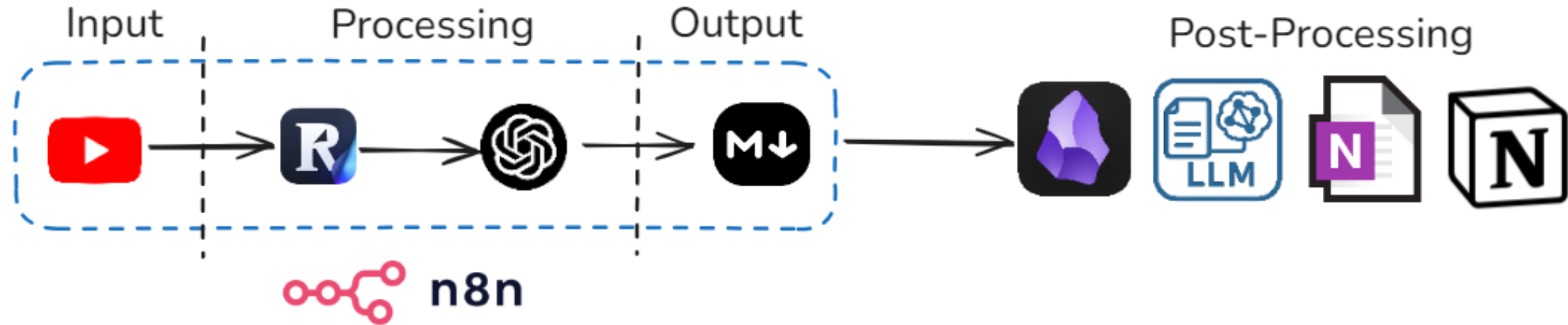
- Context is very important.

Fabric: Human Augmentation Framework

- Open-source framework.

- Unlike traditional AI applications, Fabric focuses on solving the integration problem.

- Using AI prompts (called Patterns) for real-world tasks.

Content Distillation

Workflow Example

01

Chain of Prompts

Three prompts to the AI to Extract Wisdom, Summarise and provide timestamps.

02

Processing

Store for reading later and later reference. Transcript sent to ChatGPT.

03

Output

AI outputs using Markdown. Lightweight markup language that uses plain text.
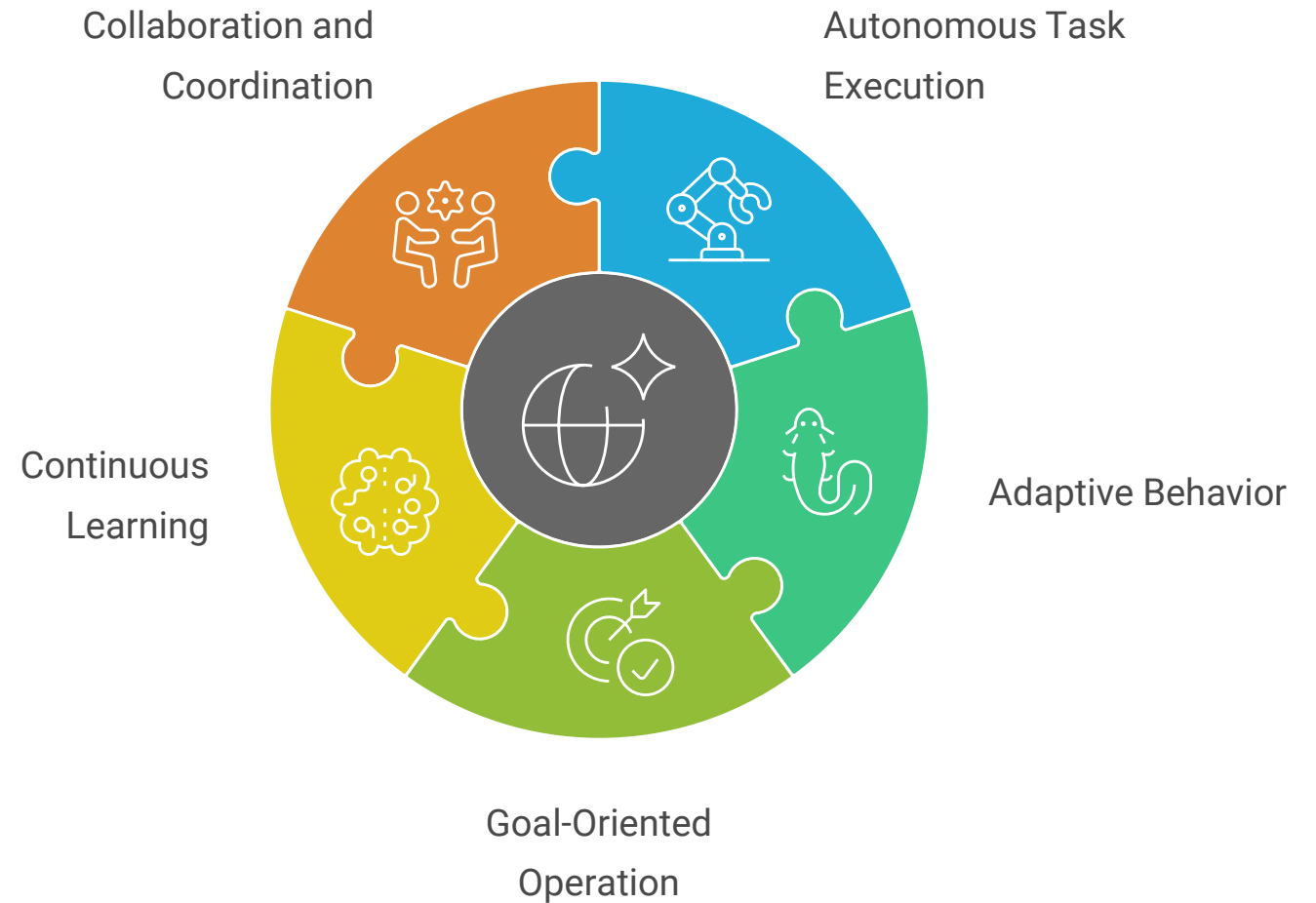
04

Post-Processing

Store anywhere, reference or distil further

Agentic AI

- LLMs are trained to use tools to complete their tasks.

- Allowing the LLM to understand what each tool is for and when to use it.

- Perceive, reason, plan, and act in complex environments.

Collaboration and Coordination

Autonomous Task Execution

Continuous Learning

Adaptive Behavior

Goal-Oriented Operation

Nomad Threat Intelligence Framework

- Comprehensive open source threat intelligence framework.

- Agentic AI workflow with Human in the Loop.

- Still in early development stages.

- Prototypes with ChatGPT Agent and Manus.ai currently run as the Orchestrator.

Threat Intelligence Agents

RSS Feed Agents
Monitor threat intelligence feeds and vulnerability databases.

Process Twitter/X, Reddit, and specialized forums for threats.
Social Media Agents

Video Content Agents
Analyze YouTube security channels and conference talks for insights.

Gather information from traditional media and security publications.
News Aggregation Agents

Technical Source Agents
Monitor GitHub repositories, security advisories, and CVE databases.

Orchestrator

Manus.ai

- Manus is a true agentic product.

- Designed to operate independently.

- High level instructions in natural language.

- Can direct multiple "Wide Research" agents to conduct concurrent work.

- Scheduled to run weekly.
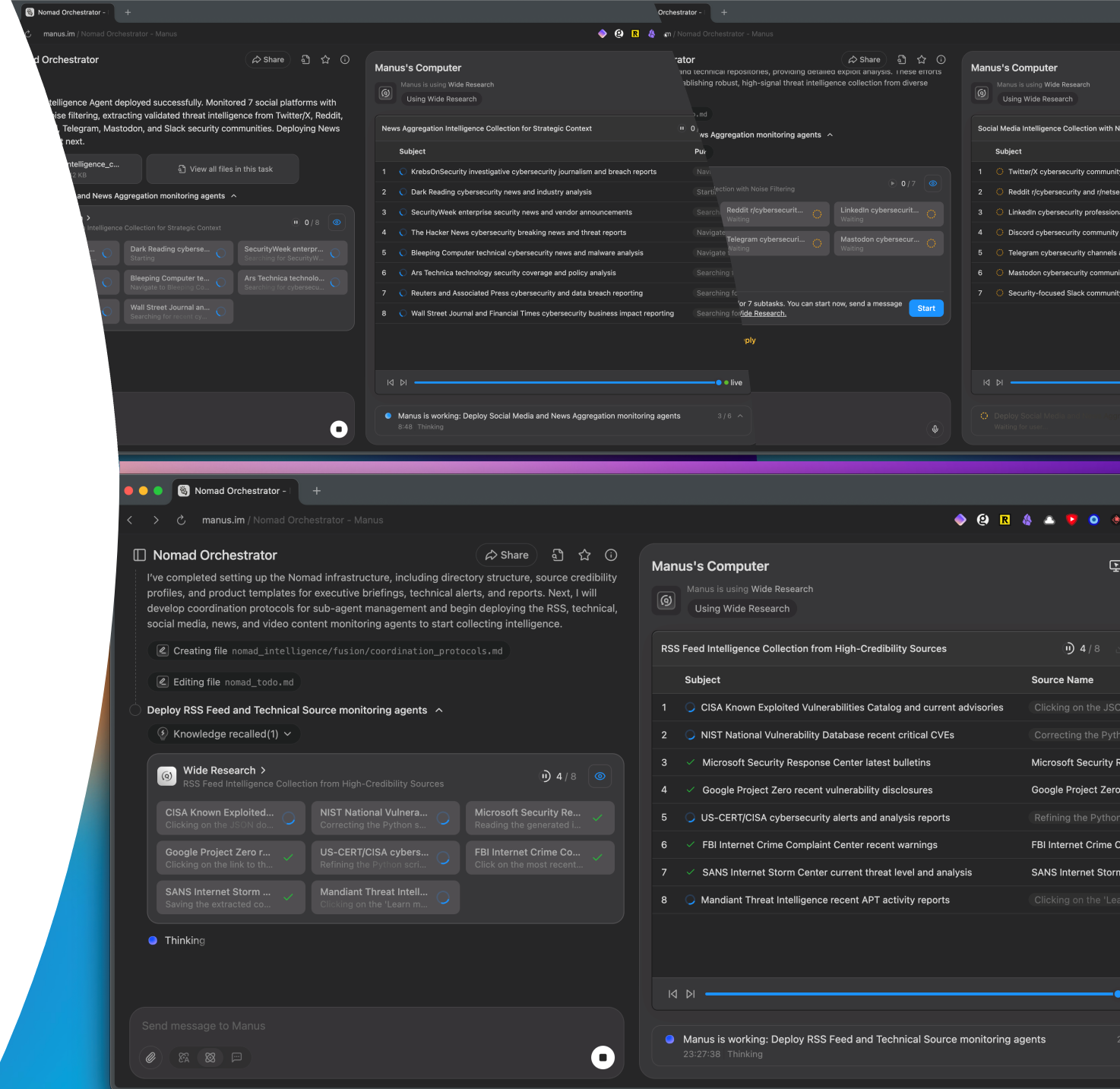
Top Tips

- Use Markdown – it is just plain text

- Start small and scale up

- Draft a prompt, give it context – Get the AI to polish the prompt

- Context is king

- Brainstorm with the AI

Links & References

Fabric: Human Augmentation Framework (https://github.com/danielmiessler/Fabric)

Readwise Reader – Read-it-later (https://readwise.io/read)

n8n Automation platform (https://n8n.io)

Obsidian Markdown Note Taker (https://obsidian.md)

Linkedin - www.linkedin.com/in/euanmcgregor

Website – https://euan.scot

These materials are for training purposes only and are not intended to be a comprehensive review of all developments in the law and practice, or to cover all aspects of those referred to. Please take legal advice before applying anything contained in these materials to specific issues or transactions. For more information please contact the presenters or your usual contact.