



ฉบับ 1.0 · สิงหาคม 2026

CONDUCTOR

ประมวลองค์ความรู้ AI Orchestration

จากโปรโตคอลถึงอาชีพ — คู่มือฉบับสมบูรณ์

เอกสารนี้สังเคราะห์แกนหลักจากคลัง 67 แหล่งในระบบต้นทาง แล้วขยายด้วยแหล่งเปิดอิสระปี 2024–2026 ว่าด้วย MCP, A2A, MAS, ธรรมชาติบาล, HITL และตลาดแรงงาน ไม่ใช่คำแนะนำการจ้างงานเฉพาะบุคคล และไม่ใช้คู่มือกฎหมาย

สารบัญ

- 00 · วิธีอ่าน
- 01 · ห้าแกนหลัก
- 02 · กายวิภาคของวาทกตร
- 03 · ปูเส้นทางอาชีพ
- 04 · วัดความเข้ากับตัวบุคคล
- 05 · คิดค้นอาชีพที่จับมือกับ AI

06 · แล็บแปดสัปดาห์

07 · อภิธานและแหล่งอ้างอิง

08 · บทส่งท้าย

๐๐

วิธีอ่าน

อ่านบทนำและแกนทั้งห้าก่อน หากต้องการเข้าใจภูมิทัศน์

ทำแบบวัดความเข้ากันในแอป แล้วค่อยอ่านเส้นทางอาชีพตามอาร์คไทป์ที่ได้

อย่าเก็บเฟรมเวิร์กเป็นเป้าหมาย เก็บวงที่วิ่งบนข้อมูลจริงเป็นเป้าหมาย

บทคิดค้นอาชีพใช้ได้แม้คุณจะไม่เรียกตัวเองว่าวิศวกร

แหล่งอ้างอิงอยู่ท้ายเล่ม เปิดเมื่อต้องการตรวจสอบ ไม่ต้องท่อง

โลกกำลังก้าวข้ามขีดของ AI ตัวเดียวไปสู่ระบบนิเวศการทำงานร่วมกัน ความท้าทายต่อไปไม่ใช่การทำให้โมเดลฉลาดขึ้นเป็นหลัก แต่คือการกำกับจังหวะ — ร้อยเรียง ควบคุมสิทธิ์ รับมือข้อขัดแย้ง และออกแบบจังหวะที่คุณเข้าแทรก

วาทกกรไม่เล่นทุกเครื่อง วาทกกรได้ยินทั้งวง รู้ว่าใครควรเข้า รู้ว่าเมื่อไหร่ต้องเจียบ และรับผิดชอบเสียงที่ออกจากห้อง

อาชีพที่จับมือกับ AI อย่างยั่งยืนมีแกนที่เครื่องทำแทนไม่ได้: ดุลยพินิจ ความรับผิดชอบ และการซ่อมความเข้าใจหลังความผิดพลาด ถ้าตำแหน่งของคุณไม่มีสามอย่างนี้ อีกไม่นานมันจะกลายเป็นปุ่ม

01

ห้าแกนหลัก

01

กระบวนทัศน์มัลติเอเจนต์และโปรโตคอล

The Multi-Agent Paradigm & Protocols

ยุคถัดไปไม่ใช่โมเดลเดี่ยวที่ฉลาดขึ้น แต่คือวงดนตรีของเอเจนต์ที่แต่ละตัวมีหน้าที่เฉพาะ และมีวาทกรคอย จังหวะ โปรโตคอล และจุดหยุด

LLM ตัวเดียวเก่งเรื่องภาษา แต่ฟังเรื่องงานยาว งานกับซ้อน และงานที่ต้องจำสถานะ Multi-Agent System (MAS) แยกหน้าที่ ประกาศเจตนา และรวมผลผ่านออร์เคสตรา — นี่คือหัวใจของคำว่า conductor

ทำไมโมเดลเดี่ยวถึงไม่พอ

โมเดลภาษาขนาดใหญ่เป็นเครื่องทำนายโทเคน ไม่ใช่ระบบปฏิบัติการของงาน ความผิดพลาดสะสมเมื่องานยาว บริบทล้น และไม่มีจุดตรวจที่เป็นทางการ การโยนทุกอย่างให้โมเดลเดี่ยวเท่ากับให้มือไวโอลินคนเดียวเล่นซิมโฟนี ทั้งเพลง

งานจริงในองค์กรมีหลายชนิดข้อมูล หลายสิทธิ์ และหลายจังหวะเวลา ราคาหุ้น ข่าว งบการเงิน นโยบายความเสี่ยง และคำตัดสินของมนุษย์ ไม่ควรอยู่ในหัวเดียวกันโดยไม่มีขอบเขต

วาทกรไม่ได้เล่นทุกเครื่อง แต่กำหนดจังหวะ ใครเข้าเมื่อไหร่ และเมื่อไหร่ที่วงต้องเงียบเพื่อฟังเดี่ยว

สถาปัตยกรรมแบบกราฟและสถานะ

LangGraph ได้รับความนิยมเพราะมองเวิร์กโฟลว์เป็นกราฟที่มีโหนด ขอบ และสถานะร่วม เอเจนต์หยุดพัก รอ การตัดสินใจของมนุษย์ แล้วทำงานต่อโดยไม่ลืมบริบท — นี่คือ durable execution ไม่ใช่แชทครั้งเดียว

CrewAI ใช้คำอุปมาที่งานตามบทบาท เหมาะกับการสร้างต้นแบบเร็ว AutoGen ของไมโครซอฟต์ใช้รูปแบบ สนทนาและการถกเถียงระหว่างเอเจนต์ Kimi Agent Swarm และเฟรมเวิร์กผู้อื่นแบ่งงานขนานแล้วรวมผล กฎที่ใช้ได้จริง: เริ่มด้วย 2–3 เอเจนต์ที่มีขอบเขตชัด อย่าเริ่มด้วยลำดับชั้น 20 ตัว ใส่ recursion limit และจำกัด การมอบหมายงาน มิฉะนั้นจะเล่นวนไม่จบ

MCP – พอร์ต USB-C ของโมเดล

Model Context Protocol (Anthropic, w.ย. 2024) เป็นมาตรฐานเปิดให้แอป AI ต่อกับไฟล์ ฐานข้อมูล เครื่องมือ และเวิร์กโฟลว์โดยไม่ต้องเขียนอแดปเตอร์ใหม่ทุกคู่ โครงสร้างคล้าย Language Server Protocol: มีโฮสต์ ไคลเอนต์ และเซิร์ฟเวอร์

สเปกล่าสุดรองรับ structured tool output, elicitation (ถามผู้ใช้แบบเป็นระบบ), OAuth resource indicators และ streamable HTTP ในเดือน ธ.ค. 2025 Anthropic มอบ MCP ให้ Agentic AI Foundation ภายใต้ Linux Foundation ร่วมกับ Block และ OpenAI

วาทกรต้องรู้ว่า MCP แก้ปัญหาการเชื่อมต่อ ไม่ได้แก้ปัญหารรรมากิบาลโดยกำเนิด การมีพอร์ตมาตรฐานไม่ได้ แปลว่าทุกสายที่เสียบเข้าไปปลอดภัย

A2A – เอเจนต์คุยกับเอเจนต์

Agent2Agent Protocol เปิดตัวโดย Google เม.ย. 2025 และส่งต่อให้ Linux Foundation ภายในปีแรกมีองค์กรสนับสนุนเกิน 150 ราย รวม AWS, Microsoft, IBM, Salesforce, SAP, ServiceNow

A2A ให้เอเจนต์ต่างผู้ผลิตค้นพบกัน สื่อสาร และส่งมอบงานโดยไม่เปิดไส้ใน MCP เชื่อมโมเดลกับเครื่องมือ A2A เชื่อมเอเจนต์กับเอเจนต์ ทั้งคู่เสริมกัน ไม่ใช่คู่แข่ง

โปรโตคอลอื่นในสนามเดียวกัน: ACP (IBM) และ ANP (ชุมชน) วาทกยกรไม่จำเป็นต้องเชิยร์ค่าย แต่ต้องอ่านแผนที่ และรู้ว่าองค์กรตัวเองพูดภาษาไหน

การจัดการข้อขัดแย้ง — MPAC และเจตนา

เมื่อเอเจนต์หลายตัวทำงานกับ โปรโตคอลอย่าง MPAC (Multi-Principal Agent Coordination) บังคับให้ประกาศเจตนาก่อนลงมือ ทำงานกับ ระบบเตือนและสามารถดึงมนุษย์เข้ามา

นี่คือสกลหลักของวาทกยกร: ออกแบบ intent schema, overlap detector และ escalation path ไม่ใช่แค่เขียนพรอมต์ให้แต่ละตัวสุภาพ

วงที่ดีมีกตทว่าใครถือไม้เมื่อไหร่ วงที่แย่คือทุกเครื่องเล่นพร้อมกันแล้วโทษว่าโมเดลโง่

สรุป: คิดเป็นวง ไม่คิดเป็นพระเอกตัวเดียว · สถานะต้องอยู่ภายนอกห้วโมเดล — กราฟ, checkpoint, หน่วยความจำ · MCP เชื่อมเครื่องมือ A2A เชื่อมเอเจนต์ ไม่มีอันใดแทนธรรมาภิบาล · ประกาศเจตนาก่อนลงมือ งานกับต้องมีทางออกสู่คน

บูรณาการองค์กรและสถาปัตยกรรมบริบท

Enterprise Integration & Context Architecture

ความฉลาดของโมเดลไม่ใช่ขอบของงานจริง ขอบคือสิทธิ์ บริบทเฉพาะองค์กร หน่วยความจำ และต้นทุนต่อคำขอ

ระบบที่ขึ้นโปรดักชันได้ต้องดึงได้เฉพาะสิ่งที่ผู้ใช้คนนั้นมีสิทธิ์ ต้องมีชั้นบริบทของความรู้เจียบในองค์กร และต้องจำได้โดยไม่เพาโทเคนทุกครั้ง

API และการควบคุมสิทธิ์

การต่อ AI กับระบบเดิมต้องผ่าน API ที่รัดกุม Role-Based Access Control (RBAC) และ Personal Access Tokens ต้องไหลผ่านเอเจนต์ ไม่ใช่เข้าไป MCP server ที่ดึงข้อมูลได้ทุกอย่างเท่ากับเปิดคลังให้ทุกคนที่ถือแชท
หลักการทอง: สิทธิ์ของเอเจนต์ต้องไม่เกินสิทธิ์ของมนุษย์ที่เรียกมัน ผู้ดูแลเห็นทั้งหมด ผู้เขียนเห็นเฉพาะงานของตน อย่าสร้าง ‘ซูเปอร์ยูสเซอร์เงา’ เพื่อความสะดวกของเดโม

PAT, short-lived credentials, least privilege และ audit log คือสกลของวากยกรพอ ๆ กับพรมณ์

Context Layer / Context Lakehouse

องค์กรต้องมีชั้นบริบทที่เก็บความรู้เฉพาะ — นโยบาย ศัพท์ภายใน เหตุผลที่เคยตัดสินใจ แบบอย่างที่ดีและไม่ดี RAG ดึงจากชั้นนี้เพื่อลดการมั่ว

ปี 2026 คำว่า context engineering กว้างกว่า RAG: ครอบคลุมสิ่งที่โมเดลเห็นตอนอนุมานทั้งหมด ทั้งคำสั่ง ดึงข้อมูล หน่วยความจำ ผลจากเครื่องมือ และงบโทเคน รายงานผู้นำด้านข้อมูลระบุว่าร้อยละ 77 เห็นว่า RAG อย่างเดียวไม่พอสำหรับโปรดักชัน

สีกาลยกรพื้นฐาน (LangChain): Write, Select, Compress, Isolate เขียนสิ่งที่ควรจำ เลือกสิ่งที่ควรเข้าหน้าต่าง บับสิ่งที่ยาว แยกสิ่งที่อันตรายไม่อยู่ปนกัน

หน่วยความจำ ต้นทุน และจังหวะเรียลไทม์

Redis และชั้นแคชเชิงความหมายเก็บคำตอบที่คล้ายกัน ประวัติสนทนา และสถานะชั่วคราว ทำให้สลับงานได้โดยไม่ลิม และไม่จ่ายโทเคนซ้ำ

วากยกรคิดเป็นต้นทุนต่อผลลัพธ์ ไม่ใช่ต่อความว้าว เอเจนต์ขนานที่เรียกโมเดลแพ่งสักรอบโดยไม่จำเป็นคือวงที่เล่นผิดห้อง

แยกหน่วยความจำเป็นสามชั้น: episodic (เกิดอะไรขึ้น), semantic (รู้อะไร), procedural (ทำอย่างไร) อย่าเททั้งหมดลงเวกเตอร์เดียวแล้วเรียกว่าความจำ

จากพรมณ์สู่ระบบ

Prompt chaining ยังมีที่ — ใช้ร้อยขั้นตอนที่คาดได้ เช่น รับเรื่องลูกค้า → จัดประเภท → ดึงนโยบาย → ร่าง → ตรวจ → ส่ง แต่เมื่อมีเงื่อนไขแตกแขนง จุดอุมัติ และสถานะค้างคั้ง ต้องย้ายไปกราฟ

สิ่งที่องค์กรซื้อจริงไม่ใช่เดโมแชท แต่เป็นท่ที่วัดได้ มีเจ้าของ มีสื่อ และมีจุดหยุด

สรุป: สิทธิของเอเจนต์ = สิทธิของคนที่เรา ไม่มากกว่า · RAG เป็นเทคนิคหนึ่งในบริบท ไม่ใช่สถาปัตยกรรมทั้งก้อน · จำเป็นขึ้น ไม่เทรวม แคชสิ่งที่ซ้ำ · ต้นทุนต่อผลลัพธ์คือเมตริกของวาทก

ธรรมาภิบาล จริยธรรม และช่องโหว่ของโปรโตคอล

Governance, Ethics & Protocol Gaps

เมื่อเอเจนต์มีอิสระ ความเสี่ยงเลื่อนจากระดับแอปไปสู่ระดับองค์กรและระดับชาติ โปรโตคอลเชื่อมต่อเก่ง แต่ยังไม่มิดธรรมาภิบาลโดยกำเนิด

MCP และ A2A ไม่มาพร้อมกลไกโหวต การเก็บความเห็นต่าง หรือการส่งเรื่องให้มนุษย์แบบเป็นระบบ วากยกรจึงต้องออกแบบขึ้นนี้เอง ไม่เช่นนั้นจะเร็วแต่ไร้ความรับผิดชอบ

ช่องว่างโดยกำเนิด

โปรโตคอลปัจจุบันเก่งเรื่องการต่อสาย ไม่เก่งเรื่องการตัดสินใจร่วม ไม่มีการโหวตของเอเจนต์ ไม่มีการเก็บ dissent ไว้เป็นหลักฐาน และไม่มีทางส่งเรื่องให้คนที่ออกแบบมาเป็นค่าเริ่มต้น

ถ้าไม่สร้างขั้นนี้ ระบบจะเลือกทางที่ ‘สั้น’ ที่สุดเสมอ — ซึ่งมักคือทางที่ไม่มีใครค้าน ไม่มีใครจำ และไม่มีใครรับผิดชอบ วากยกรที่ดีเก็บบันทึกความเห็นต่างไว้แม้ทางที่เลือกจะต่างออกไป เพราะวันหนึ่งจะต้องอธิบายว่าทำไม

ETHOS และธรรมาภิบาลไร้ศูนย์กลาง

กรอบ ETHOS เสนอใช้ Web3, blockchain, smart contracts และ DAO สร้างทะเบียนควบคุมเอเจนต์แบบกระจายศูนย์ เพื่อตรวจสอบความน่าเชื่อถือ แบ่งความเสี่ยง และควบคุมพฤติกรรมในระดับที่ใหญ่กว่าองค์กรเดียว (Chaffer et al., arXiv 2412.17114)

ไม่ใช่ทุกองค์กรต้องขึ้นเชน แต่แนวคิดมีประโยชน์: ตัวตนของเอเจนต์ต้องตรวจสอบได้ นโยบายต้องเป็นรหัสที่ตรวจสอบได้ และการลงโทษ/จำกัดขอบเขตต้องไม่ขึ้นกับทีมเดียวที่ล้ม

ในทางปฏิบัติ องค์กรส่วนใหญ่เริ่มจากทะเบียนเอเจนต์ภายใน, นโยบายเป็นรหัส, และคณะกรรมการที่ยกเลิกสิทธิ์ได้ในชั่วโมง ไม่ใช่ในไตรมาส

ภัยคุกคามรูปแบบใหม่

Indirect prompt injection อยู่หัวตาราง OWASP LLM Top 10 แฮกเกอร์ซ่อนคำสั่งในหน้าเว็บ ไฟล์ หรือตัวซอฟต์แวร์ เมื่อเอเจนต์ไปอ่าน มันทำตามคำสั่งที่แอบมา

เอเจนต์ที่มี agency สูงเสี่ยงกว่าแฮก เพราะมันไม่เพียงพูดผิด แต่ทำผิด — ส่งเมล ย้ายเงิน แก่สิทธิ์ เปิดประตู การป้องกันที่วากยกรออกแบบได้: แยกบริบทเครื่องมือออกจากคำสั่งระบบ, ทำ allowlist ของการกระทำ, ใส่จุดอนุมัติก่อนผลที่ย้อนกลับไม่ได้, และอย่าให้เอเจนต์เชื่อข้อความจากภายนอกเท่ากับนโยบายภายใน

ธรรมาภิบาลในฐานะจังหวะ ไม่ใช่เอกสาร

นโยบายที่อยู่ในวิกิและไม่อยู่ในรันไทม์คือพรอพบนเวที ธรรมาภิบาลที่ทำงานได้คือเกตในกราฟ: ถ้าความมั่นใจต่ำ ถ้าข้อมูลส่วนบุคคล ถ้าเงิน ถ้าชื่อเสียง — หยุด

วัดสิ่งที่วัดได้: อัตราการส่งต่อให้คน, อัตราการถูกตีกลับ, จำนวนการกระทำที่ย้อนกลับไม่ได้โดยไม่มีลายเซ็น, เวลาเฉลี่ยตั้งแต่พบความผิดปกติถึงการถอดปลั๊ก

สรุป: โปรโตคอลเชื่อมต่อ $\neq$ โปรโตคอลธรรมาภิบาล · เก็บ dissent ไว้เป็นทรัพย์สิน ไม่ใช่ขยะ · Injection ทางอ้อมคือภัยหลักของเอเจนต์ที่อ่านโลกภายนอก · นโยบายต้องอยู่ในรันไทม์ ไม่ใช่แค่ในวิกิ

มนุษย์ในรูปและจิตวิทยาการเรียนรู้

Human-in-the-Loop & The Research of How

ระบบที่ใช้งานจริงมีจุดให้คนอนุมัติ แก่ และหยุดได้เสมอ สิ่งสำคัญไม่ใช่ความผิดพลาด แต่คือเส้นทางหลังจากนั้น

HITL ไม่ใช่ปุ่มตกแต่ง แต่เป็นสถาปัตยกรรม การซ่อมความเข้าใจผิดสร้างความไว้วางใจที่แม่นยำ การรับมือหรือหลีกเลี่ยงสร้างแค่ความโล่งชั่วคราว

จุดตรวจรันไทม์

LangGraph มี interrupt() ให้กราฟหยุดที่โหนดที่กำหนด รอคำตอบของคน แล้วทำงานต่อจาก checkpoint รูปแบบที่ใช้บ่อย: approval gate, เกณฑ์ความมั่นใจ, และวงฟีดแบ็ก

แยกสองแบบให้ชัด: โมเดลเลือกที่จะถามคน กับ กราฟบังคับให้ถามคน อย่างหลังใช้กับสิ่งที่ย้อนกลับไม่ได้

แดชบอร์ดอนุมัติต้องแสดงเจตนา ข้อมูลที่ใช้ ผลกระทบ และทางเลือก ไม่ใช่แค่ปุ่มใช่/ไม่ใช่บนข้อความคลุมเครือ

The Research of How — เส้นทางหลังความผิด

เมื่อนุษย์ใช้ AI แล้วผลไม่ตรงคาด (mismatch / prediction error) คำถามที่สำคัญไม่ใช่ ‘พลาดไหม’ แต่ ‘เดินต่ออย่างไร’

ถ้ามีที่ว่างให้ซ่อมความเข้าใจ — อธิบาย แก้ขอบเขต ลองใหม่ — โมเดลของคนต่อระบบจะละเอียดขึ้น ความไว้วางใจจะตรงกับความสามารถจริง

ถ้าหนีหรือรับมือ จะได้แค่ความโล่งชั่วคราว ไม่เกิดการเรียนรู้ แล้วพลาดแบบเดิมซ้ำในวันที่ไม่มีคนเฝ้า

ภาษาที่โมเดลอธิบายตัวเอง vs ความจริงตอนรัน

AI มักมั่นใจในคำอธิบายตนเอง (self-model language) แต่พฤติกรรมจริงอาจไม่ตรง ความขัดแย้งนี้คือเครื่องมือให้คนเห็นขอบเขตของกล่องดำ

วากยกรไมถามแค่ ‘เธอทำได้ไหม’ แต่ตั้งงานสอบที่พิสูจน์ได้ แล้วเทียบคำพูดกับร่องรอยการรัน

Error ที่มองเห็นดีกว่าความสำเร็จที่อธิบายไม่ได้

สถาปัตยกรรมของการหยุด

ประโยคที่ใช้ในแหล่งต้นทางยังใช้ได้: เครื่องมือที่หยุดไม่ได้ ไม่ใช่เครื่องมืออีกต่อไป

ระบบต้องรู้จุดที่ตัวเองจัดการไม่ได้ — ความรับผิดชอบทางกฎหมาย การตัดสินใจที่กระทบชีวิต การขัดกันของค่านิยม — แล้วส่งต่อให้คนอย่างสง่างาม ไม่ใช่แอบทำต่อ

Human handoff ที่ดีมีบริบทครบ ทางเลือกชัด และไม่โทษผู้รับว่ามาช้า

สรุป: HITL คือสถาปัตยกรรม ไม่ใช่ปุ่มตกแต่ง · ซ่อมดีกว่าหนี ความไว้วางใจต้องตรงความสามารถ · อย่าเชื่อคำอธิบายตนเองโดยไม่เทียบร่องรอยรัน · ออกแบบการหยุดก่อนออกแบบความเร็ว

การเปลี่ยนผ่านอุตสาหกรรมและอาชีพ

Industry Transformation & Future Careers

องค์กรไม่ได้ต้องการแค่คนเขียนโค้ดเอเจนต์ แต่ต้องการคนที่คิดเป็นระบบ แตกโจทย์ได้ และดูแลวงให้ปลอดภัย
ทักษะนี้มีชื่อแล้ว: AI Agent Orchestrator

อาชีพใหม่ไม่ได้เกิดจากการตั้งชื่อเท่ แต่จากช่องว่างที่ระบบจริงต้องการคนยืน — ระหว่างเอเจนต์กับเอเจนต์
ระหว่างเอเจนต์กับคน และระหว่างวงกับความรับผิดชอบ

การศึกษา — Multi-AI Teaching Orchestra

ในระบบอย่าง Google Classroom มีการออกแบบวงสอนที่เอเจนต์รับบทนักเรียนและครูเฉพาะทาง เช่น Socratic, Assessor, Enricher ภายใต้กฎ Sequence Lock — ห้ามแย่งกันสอน มนุษย์ตรวจและอนุมัติผ่านแดชบอร์ด
บทเรียนสำหรับวาทกรรมทุกวงการ: บทบาทต้องไม่ทับจังหวะ และคนต้องเห็นพาร์ติเตอร์ ไม่ใช่แค่ผลลัพธ์สุดท้าย

ดนตรีและศิลปะ

มีหุ่นยนต์วาทกรรมที่คุมวงมนุษย์ได้จริง เฟรมเวิร์กอย่าง MG-Former แปลงจังหวะเพลงเป็นการเคลื่อนไหวสามมิติ ทฤษฎี TSCP (Trans-Semiotic Co-Creation Protocols) อธิบายการร่วมสร้างระหว่าง AI กับ AI ที่พัฒนา
กฎไวยากรณ์ใหม่เอง

นี่ไม่ใช่แค่เกร็ดศิลปะ แต่เป็นแบบจำลอง: เมื่อเอเจนต์ร่วมสร้าง ต้องมีไวยากรณ์ร่วม และต้องมีคนรับผิดชอบต่อผลงานที่ออกสู่โลก

ตลาดแรงงาน 2025–2030

Future of Jobs Report 2025 ของ WEF สํารวจนายจ้างกว่า 1,000 ราย ทักษะที่โตเร็วสุดคือ AI และบิกดาต้า
ตามด้วยเครือข่าย/ไซเบอร์ และความเข้าใจเทคโนโลยี บทบาทที่โตเร็วเป็นกลุ่มเทคโนโลยี แต่ทักษะมนุษย์ — คิดวิเคราะห์ ยืดหยุ่น นำการเปลี่ยนแปลง — ยังเป็นแกน

บทวิเคราะห์ปี 2026 ชี้ว่าผลผลิตมาจากการจัดวง ไม่ใช่การแทนที่คน Eightfold และผู้ปฏิบัติจำนวนมากเรียก AI agent orchestration ว่าหนึ่งในงานสำคัญของปี

ตลาดงานสหรัฐช่วงกลางปี 2026 ระบุช่วงค่าตอบแทน orchestration โดยประมาณ 1.45–1.84 แสนดอลลาร์
ต่อปี (ขึ้นกับเมืองและระดับ) ในเอเชียตะวันออกเฉียงใต้บทบาทนี้ยังใหม่ — ผู้ที่สร้างพอร์ตโฟลิโอก่อนตลาดอึมครว
ได้เปรียบ

ทักษะที่ตลาดซื้อจริง

คิดเชิงระบบและแตกโจทย์ธุรกิจเป็นงานย่อย

ออกแบบเวิร์กโฟลว์คน-เครื่อง รวมจุดอนุมัติ

แปลความรู้ของผู้เชี่ยวชาญให้เอเจนต์ใช้ได้

นำการเปลี่ยนแปลงและสร้างความไว้วางใจที่ตรงความจริง

ออกแบบบรรณาภิบาลที่รันได้ ไม่ใช่แค่พูดได้

สรุป: อาชีพวาทกยกรคือช่องว่างระหว่างวงกับความรับผิดชอบ · Sequence lock มีประโยชน์นอกห้องเรียน · ตลาดซื้อการคิด
เชิงระบบมากกว่าการท่องชื่อเฟรมเวิร์ก · อาชีพใหม่เกิดจากช่องว่างที่วัดได้ ไม่ใช่จากสไลด์

02

กายวิภาคของวาทยกร

AI Agent Orchestrator คือคนที่แตกโจทย์เป็นบทบาท จัดวางเอเจนต์ให้เล่นร่วมกัน ออกแบบจุดหยุด และรับผิดชอบต่อผลของวง — ไม่ใช่คนที่พิมพ์โปรแกรมที่เก่งที่สุดในห้อง

ไม่ใช่ / คือ

ไม่ใช่ — แยกบอกมาสเตอร์ที่สะสมเกมเพลต

ไม่ใช่ — แค่ ML engineer ที่จูนโมเดล

ไม่ใช่ — project manager ที่ส่งต่อตัวโดยไม่แตะระบบ

ไม่ใช่ — คนที่ปล่อยเอเจนต์แล้วหวังว่าธรรมชาติจะเกิดเอง

คิดเป็นระบบ: คน เครื่อง ข้อมูล สิทธิ์ จังหวะ

แตกปัญหาได้จนแต่ละเอเจนต์มีขอบเขตที่ทดสอบได้

ออกแบบการส่งไม้และจุดที่คนต้องเข้า

วัดวงด้วยผลลัพธ์ ความปลอดภัย และต้นทุน ไม่ใช่ด้วยความว้าวของเดโม

พาร์ติเตอร์: โจทย์และสัญญา

เป้าหมายทางธุรกิจที่วัดได้

ขอบเขต สิ่งห้าม นิยามความสำเร็จ

intent schema ที่เอเจนต์ต้องประกาศก่อนลงมือ

นักดนตรี: บทบาทเอเจนต์

แต่ละตัวหนึ่งหน้าที่ หนึ่งชุดเครื่องมือ

โมเดลที่เหมาะสมกับงาน ไม่ใช่โมเดลแพงทุกที่

ทดสอบเดี่ยวก่อนเข้าวง

จังหวะ: ออร์เคสตรา

ลำดับ ขนาน เจี้ยนไฮ ลูป มีขีดจำกัด

checkpoint และสถานะอยู่นอกหัวโมเดล

sequence lock เมื่อบทบาทห้ามทับ

หู: สังเกตการณ์

ลือกเจตนา เครื่องมือ ต้นทุน ผล
 เทียบคำอธิบายตนเองกับร่องรอยรัน
 เตือนเมื่อทำงานหรือเกินงบ

ไม่หยุด: HITL และ handoff

เกตก่อนผลที่ย้อนกลับไม่ได้
 แดชบอร์ดอนุมัติที่อ่านเป็นเรื่อง
 สคริปต์ส่งต่อคนพร้อมบริบท

วันที่ของงาน

เข้า. อ่านลือกวงที่วิ่งค้างคั่น แยกสัญญาณจากเสียงรบกวน ปิดหรือลดสิทธิ์ตัวที่เดินผิด

สาย. คุยกับเจ้าของโดเมน เก็บความรู้เจียบหนึ่งขึ้นใส่ชั้นบริบท แก้ขอบเขตเอเจนต์ตามเคสจริง

บ่าย. ออกแบบหรือแก้กราฟ ใส่เกต เขียนแบบทดสอบ mismatch วัตต้นทุนต่อผลลัพธ์

เย็น. ซ่อมถอดปลั๊กหรือรีวิวเคสที่คนตักกลับ บันทึก dissent และเส้นทางซ่อม

ทักษะแกน

Systems thinking — มองคน-เครื่อง-ข้อมูล-สิทธิ์พร้อมกัน

Problem decomposition — แยกโจทย์จนทดสอบได้

Process design — เขียนจังหวะงานก่อนเลือกเครื่องมือ

Judgement & ethics — รู้ว่าเมื่อไหร่ต้องไม่ปล่อยอัตโนมัติ

ทักษะเทคนิค

Graph orchestration — LangGraph หรือเทียบเท่า สำหรับสถานะและจุดหยุด

MCP / A2A literacy — ต่อเครื่องมือและต่อเอเจนต์อย่างมีขอบเขต

Context engineering — RAG + หน่วยความจำ + จบโทเคน

Eval & observability — วัดวงได้ ไม่เดา

ทักษะองค์กร

RBAC & secrets — เอเจนต์ไม่เกินสิทธิ์คน

Change leadership — พาคนใช้วงโดยไม่ขายฝัน

Domain partnership — แปลผู้เชี่ยวชาญเป็นสัญญาณที่เครื่องใช้ได้

Cost control — วงที่แพงเกินประโยชน์จะถูกปิด

03

ปูเส้นทางอาชีพ

สายโดเมน. คนที่รู้งานจริง — ปฏิบัติการ การเงิน การศึกษา สุขภาพ กฎหมาย ศิลปะ — แต่ยังไม่ใช้วิศวกร จุดเริ่ม: เลือกงานซ้ำที่คุณทำอยู่แล้ว แล้วสร้างวง 2–3 เอเจนต์ที่ช่วยงานนั้น มีจุดให้คุณอนุมัติ

สายเทคนิค. คนที่เขียนระบบได้แล้ว อยากเลื่อนจากโมเดลเดี่ยวสู่โปรดักชันมัลติเอเจนต์ จุดเริ่ม: ย้ายแชทบอทหนึ่งตัวขึ้นกราฟ มี checkpoint, จบโทเคน, และเกตหนึ่งจุด

สายธรรมาภิบาล. คนที่มาจากความเสี่ยง กฎหมาย ตรวจสอบ หรือนโยบาย จุดเริ่ม: ทำทะเบียนเอเจนต์และรายการการกระทำที่ย้อนกลับไม่ได้ แล้วออกแบบเกตให้ทีมเทคนิคฝังในกราฟ

30 วัน — ได้ยินวง

อ่านแกนทั้งห้าในเอกสารนี้จบ และทำแล็บที่ 1–2

เลือกโดเมนเดียวที่คุณมีสิทธิ์เข้าถึงข้อมูลจริง

สร้างเอเจนต์เดี่ยวที่ดึงความรู้เฉพาะได้ โดยมีสิทธิ์จำกัด

จด mismatch ทุกครั้งที่มันพลาด — นี่คือวัฏจักร

90 วัน — ขึ้นแท่นวาทยกรเล็ก

เพิ่มเป็นวง 2–3 ตัว มีออร์เคสตราและจุดอนุมัติหนึ่งจุด

มีชั้นบริบทอย่างน้อย 10 เอกสารที่คุณคัดเอง

วัดต้นทุนต่อผลลัพธ์และอัตราการถูกคนแก้

เขียนเคสศึกษาหนึ่งหน้า เผยหรือเก็บเป็นพอร์ตโฟลิโอ

12 เดือน — เป็นเจ้าของวงในองค์กรหรือในตลาด

วงวิ่งในงานจริง ไม่ใช่เดโม มีลูกค้า มีเจ้าของ มีงบ

สอนคนอื่นให้อ่านพาร์ติเตอร์ได้

มีตำแหน่งหรือข้อเสนอที่ชื่อคล้าย orchestrator / AI operations / agent lead

เริ่มร่างอาชีพเฉพาะทางจากช่องว่างที่คุณเจอซ้ำ

36 เดือน — ตั้งสำนัก

คุณออกแบบวงได้หลายโดเมน หรือลึกมากในโดเมนเดียวจนตั้งมาตรฐาน

มีชุดอาชีพย่อยที่คุณนิยามเองและมีคนจ่าย

คุณเขียนหรือสอนสถาปัตยกรรมของการหยุดได้โดยไม่อิงค่ายเฟรมเวิร์กเดียว

พอร์ตโฟลิโอ

แผนภาพวงหนึ่งอัน: บทบาท เครื่องมือ สิกซ์ จุดหยุด

คลิปหรือบันทึก mismatch → ซ่อม → ผลดีขึ้น

ตัวเลขต้นท่อนก่อน/หลัง และสิ่งที่คนยังต้องทำ

กะเบียดเอเจนต์และนโยบายสามข้อที่รันได้

อาชีพที่คุณคิดเองหนึ่งตำแหน่ง พร้อมวันที่ของงาน

หลุมพราง

สะสมคอร์สเฟรมเวิร์กโดยไม่มีวงที่วิ่งบนข้อมูลจริง

ใช้เอเจนต์ 12 ตัวกับงานที่คนทำใน 8 นาที

วัดความสำเร็จด้วยความยาวของพรมต

ให้เอเจนต์ถือคีย์ที่กว้างกว่าที่คุณเองมี

ไม่มีทางถอดปลั๊กในวันแรกที่ขึ้นโปรดักชัน

04

วัดความเข้ากันกับตัวบุคคล

แบบวัดในแอปมี 24 ข้อ หกมิติ ให้คะแนนนิสัยไม่ให้คะแนนความรู้ ผลที่ได้คืออาร์คไทป์สำหรับเลือกสาย ไม่ใช่ใบรับรอง

คิดเชิงระบบ. มองคน เครื่อง ข้อมูล สิทธิ์ และจังหวะพร้อมกัน

แตกโจทย์. ย่อยงานจนแต่ละขั้นมีขอบเขตและทดสอบได้

อยู่กับความคลุม. เดินต่อได้โดยไม่ต้องมีสเปกสมบูรณ์

ดุษยพินิจ. รู้ว่าเมื่อไหร่ต้องหยุด ทาม หรือส่งต่อคน

ฝีมือเทคนิค. แตะเครื่องมือ โปรโตคอล และลือกได้เอง

นิสัยวากยกร. อดทนกับจังหวะ ซ่อมได้ ไม่หนีความผิด

อาร์คไทป์: วากยกรโดเมน · วากยกรระบบ · วากยกรธรรมชาติบาล · ช่างวง · ผู้ตั้งอาชีพ ทำแบบวัดในแอปแล้วบันทึกได้เมื่อเข้าสู่ระบบ

05

คิดค้นอาชีพที่จับมือกับ AI

ช่องว่างห้าช่อง — วิธีตั้งอาชีพที่จับมือกับ AI ใช้เมื่อคุณเจอช่องว่างซ้ำ ๆ ที่ยังไม่มีชื่อในใบสมัครงาน

- 1. หาจุดเจ็บที่เกิดซ้ำ.** ไม่เริ่มจากชื่อตำแหน่ง เริ่มจากเหตุการณ์ที่คนเสียเวลา เสียเงิน หรือเสียความไว้วางใจซ้ำ ๆ เพราะวงเอเจนต์ยังไม่มีคนยืนตรงนั้น
- 2. ตั้งชื่อช่องว่าง ไม่ใช่ตั้งชื่อเครื่องมือ.** ช่องว่างอยู่ระหว่างเอเจนต์กับเอเจนต์ เอเจนต์กับคน วงกับสิทธิ์ วงกับต้นทุน หรือวงกับความหมาย ถ้าพูดไม่ได้ว่าอยู่ระหว่างอะไร ยังไม่ใช่อาชีพ
- 3. เขียนวันที่ของงาน.** เข้าทำอะไร บ่ายทำอะไร วัตถุประสงค์เมื่อไร ใครส่งงานให้คุณ ใครรับงานจากคุณ ถ้าเขียนวันที่ไม่ได้ นั่นคือสไลด์
- 4. กำหนดสิ่งที่ AI ทำแทนไม่ได้ในตำแหน่งนี้.** อาชีพที่จับมือกับ AI ต้องมีแกนที่เป็นดุลยภาพ ความรับผิดชอบ หรือการเชื่อมความเข้าใจ มีฉะนั้นอีก 18 เดือนตำแหน่งจะถูกกลืน
- 5. หาผู้จ่ายก่อนหาโลโก้.** ใครเจ็บจากช่องว่างนี้จนยอมจ่ายเงิน เวลา หรืออำนาจ ถ้ายังไม่มีคนนั้น ให้ทดลอง 90 วันด้วยคนเดียว แล้วค่อยตั้งชื่อให้ดัง

บททดสอบตำแหน่ง

ถ้าถอด AI ออกแล้วยังมีงานนี้ — อาจเป็นอาชีพเดิมที่แค่ใช้เครื่องมือใหม่

ถ้าถอดคนออกแล้ววงยังรับผิดชอบได้ — นั่นไม่ใช่อาชีพ นั่นคือพีเจเออร์

ถ้าไม่มีจุดหยุดในวันที่ของงาน — อันตราย

ถ้าไม่มี mismatch ให้ซ่อม — งานนั้นตื่นเกินกว่าจะเป็นอาชีพ

สตูดิโออาชีพ

ผู้ไกล่เกลี่ยข้อขัดแย้งของเอเจนต์ / Agent Conflict Mediator

เอเจนต์หลายตัวประกาศเจตนาต่อกัน ไม่มีใครถอยไม่ และคนถูกเรียกเมื่อสายเกินไป

วันที่: อ่านคิวเจตนาที่ทับ · จัดลำดับตามนโยบายและความเร่งด่วน · ส่งเรื่องที่ค่านิยมขัดกันให้คน · ปรับสัญญาบทบาทเพื่อลดทับในรอบถัดไป

ทักษะ: MPAC / intent schema · นโยบายองค์กร · นิติธรรมเบื้องต้น · ออกแบบ escalation

เพื่อนบ้านอาชีพ: มาจาก operations, compliance, หรือ community moderation. ช่องว่าง: ช่องว่างระหว่างเอเจนต์กับเอเจนต์

บรรณารักษ์บริบท / Context Librarian

ความรู้เชิงบริหารจัดการกระจาย RAG ถึงของเก่า ของผลิตภัณฑ์ หรือของที่ไม่มีเจ้าของ

วันที่: รับเอกสารและคำตัดสินเข้าชั้นบริบท · ติดตามอายุ เจ้าของ และระดับสิทธิ์ · ตัดของทั้งหมดอายุออกจากดัชนี · ระวังคำตอบอ้างอิงแหล่งที่ยังมีชีวิต

ทักษะ: context engineering · ธรรมชาติข้อมูล · taxonomy · RBAC

เพื่อนบ้านอาชีพ: มาจาก knowledge management, บรรณารักษ์, นักวิเคราะห์นโยบาย. ช่องว่าง: ช่องว่างระหว่างวงกับความหมาย

สถาปนิกการส่งต่อคน / Human Handoff Architect

เอเจนต์ส่งเรื่องให้คนแบบไม่มีบริบท คนรับไม่รู้ว่าจะต้องตัดสินอะไร และวงไม่เรียนรู้จากคำตัดสิน

วันที่: ออกแบบสคริปต์ handoff ต่อประเภทงาน · บังคับให้เจตน์ทางเลือกและผลกระทบ · ปิดลูปคำตัดสินกลับเข้าชั้นบริบท · ซ้อมเคสยามวิกฤต

ทักษะ: HITL · UX ของแดชบอร์ดอุมัติ · incident response · การเขียนสัญญา

เพื่อนบ้านอาชีพ: มาจาก service design, incident commander, พยาบาลหัวหน้าเวร. ช่องว่าง: ช่องว่างระหว่างเอเจนต์กับคน

ผู้ออกแบบลำดับห้ามทับ / Sequence Lock Designer

เอเจนต์แย่งจังหวะ — สอนพร้อมกัน ตอบลูกค้าซ้อนกัน แก้โค้ดไฟล์เดียวกัน

วันที่: เขียนพาร์ติเตอร์ลำดับต่อโดเมน · ใส่กฎแฉลำดับในกราฟ · ตรวจจังหวะที่หลุดจากล็อก · ฝึกเจ้าของโดเมนให้อ่านพาร์ติเตอร์

ทักษะ: orchestration · pedagogy หรือ process mapping · graph design

เพื่อนบ้านอาชีพ: มาจากครูใหญ่, stage manager, release manager. ช่องว่าง: ช่องว่างระหว่างเอเจนต์กับเอเจนต์ในมิติเวลา

ผู้ตรวจเจตนา / Intent Declaration Auditor

เอเจนต์ทำก่อนพูด หรือพูดอย่าง ทำอย่าง ความรับผิดชอบไม่ทัน

วันที่: สุ่มตรวจเจตนากับร่องรอยเครื่องมือ · ตั้งเกณฑ์เจตนาที่ไม่ผ่าน · รายงานช่องว่าง self-model กับ runtime · เสนอแก้ไข

ทักษะ: eval · audit · prompt/spec writing · forensics เบื้องต้น

เพื่อนบ้านอาชีพ: มาจาก internal audit, QA, นักข่าวข้อมูล. ช่องว่าง: ช่องว่างระหว่างคำพูดกับมือ

ผู้ดูแลแคชเชิงความหมาย / Semantic Cache Steward

วงแพ่งและซ้ำ หรือแยกว่านั้น — เสริมคำตอบเก่าในบริบทใหม่

วันที่: กำหนดนโยบายอายุแคชต่อชนิดคำถาม · สร้างเมตริกนโยบายหรือสิทธิ์เปลี่ยน · วัดอัตราฉีกกลางและความเสี่ยงของคำตอบค้าง · ประสานกับบรรณารักษ์บริบท

ทักษะ: Redis / cache · ความเป็นส่วนตัว · ต้นทุนโทเคน · การประเมินความคล้าย

เพื่อนบ้านอาชีพ: มาจาก SRE, data ops. ช่องว่าง: ช่องว่างระหว่างวงกับต้นทุน/ความสด

เจ้าหน้าที่รักษาความเห็นต่าง / Dissent Preservation Officer

ระบบเลือกทางลื่นที่สุด ความเห็นที่ไม่ชนะหายไป วันอธิบายจึงอธิบายไม่ได้

วันที่: ออกแบบที่เก็บ dissent · บังคับให้การสรุปไม่ลอบทางที่ไม่ถูกเลือก · เตรียมบันทึกสำหรับคณะกรรมการและผู้ตรวจสอบ · สอนวงให้แยก ‘สรุป’ กับ ‘ลบ’

ทักษะ: ธรรมชาติบาล · จดหมายเหตุ · นโยบาย · การเขียน

เพื่อนบ้านอาชีพ: มาจากเลขาคณะกรรมการ, นักจดหมายเหตุ, ombuds. ช่องว่าง: ช่องว่างระหว่างวงกับความรับผิดชอบในระยะยาว

ผู้เรียบเรียงโซ่พรมต / Prompt Chain Composer

งานคาดได้แต่หลายชั้น ถูกโยนให้เอเจนต์อิสระแล้วพังเพราะเกินอิสระ

วันที่: แยกงานที่ควรเป็นโซ่กับงานที่ควรเป็นกราฟ · เรียบเรียงท่อบริการลูกค้าหรือคอนเทนต์ · ใส่จุดตรวจคุณภาพระหว่างท่อน · ส่งมอบเป็นสกออร์ทที่ไม่ผูกค้ายเดียว

ทักษะ: prompting · process · eval · การเขียน

เพื่อนบ้านอาชีพ: มาจาก copy chief, operations writer, BA. ช่องว่าง: ช่องว่างระหว่างงานคาดได้กับงานแตกแขนง

ผู้กลั่นความรู้เจียบ / Tacit Knowledge Distiller

ผู้เชี่ยวชาญทำได้แต่พูดไม่ได้ เอเจนต์จึงเรียนจากเอกสารผิว

วันที่: สังเกตผู้เชี่ยวชาญตอนตัดสินใจ · แปลงเป็นกรณี ขอบเขต และข้อห้าม · ตรวจสอบผู้เชี่ยวชาญว่าเพี้ยนหรือไม่ · ส่งเข้าชั้นบริบท

ทักษะ: สัมภาษณ์เชิงลึก · cognitive task analysis · การเขียนกรณี

เพื่อนบ้านอาชีพ: มาจากนักมานุษยวิทยาองค์กร, coach, ครูฝึกงาน. ช่องว่าง: ช่องว่างระหว่างหัวคนกับชั้นบริบท

สถาปนิกการหยุด / Stop-Architecture Designer

วงเร็วขึ้นเรื่อย ๆ แต่ไม่มีใครออกแบบว่าจะบออย่างไรเมื่อผิดชนิด

วันที่: จำแนกความล้มเหลวที่หยุดได้/ต้องส่งคน/ต้องถอดปลั๊ก · ฝังสวิตช์ในกราฟและในสิทธิ์ · ซ้อมและจับเวลาการถอดปลั๊ก · รายงานต่อผู้บริหารเป็นความสามารถของระบบ ไม่ใช่ความซ้ำซาก

ทักษะ: safety engineering · incident · IAM · orchestration

เพื่อนบ้านอาชีพ: มาจาก safety officer, SRE, นักบินฝึกซ้อมฉุกเฉิน. ช่องว่าง: ช่องว่างระหว่างความเร็วกับขอบเขต

วาทยกรต้นทุน / Agent Cost Conductor

วงใช้โมเดลแพงทุกท่อน ไม่มีใครต้องบต่อผลลัพธ์

วันที่: ตั้งงบต่อเวิร์กโฟลว์ · จัดโมเดลถูก/แพงตามความเสี่ยงของท่อน · ไล่ล่าลูบที่เรียกซ้ำ · รายงานต้นทุนคู่กับคุณภาพ ไม่แยกสไลด์

ทักษะ: FinOps · routing · eval · การเจรจา

เพื่อนบ้านอาชีพ: มาจาก FinOps, procurement, platform PM. ช่องว่าง: ช่องว่างระหว่างวงกับเงิน

โค้ชเส้นทางซ่อม / Repair Trajectory Coach

ทีมรับผิดชอบเพื่อความโล่ง แล้วไม่เกิดการเรียนรู้ ทั้งคนและวง

วันที่: นั่งกับทีมตอน mismatch · บังคับให้มีเส้นทางซ่อม ไม่ใช่แค่แพตช์ · ได้รับความไว้วางใจให้ตรงความสามารถใหม่ · เก็บคลังเคสซ่อม

ทักษะ: จิตวิทยาการเรียนรู้ · facilitation · eval · การเขียนเคส

เพื่อนบ้านอาชีพ: มาจากครู, therapist เชิงองค์การ, staff engineer ที่สอนเก่ง. ช่องว่าง: ช่องว่างระหว่างความผิดกับโมเดลความเข้าใจ

ผู้คัดบทเอเจนต์ / Agent Casting Director

ทุกงานถูกโยนให้โมเดลเดียวกัน บทบาทกับและสลับเปลี่ยน

วันที่: เขียนบท: หน้าที น้ำเสียง เครื่องมือ ข้อห้าม · ทดสอบเดี๋ยวก่อนเข้าวง · ปลดบทที่ไม่จำเป็น · รักษาลำดับไม่ให้แย่งซีน

ทักษะ: role design · eval · โดเมน · การเขียน

เพื่อนบ้านอาชีพ: มาจาก casting, HR design, creative director. ช่องว่าง: ช่องว่างระหว่างเจตน์กับบทบาท

นักทำแผนที่ช่องว่างโปรโตคอล / Protocol Gap Cartographer

ทีมต่อ MCP/A2A แล้วคิดว่าธรรมชาติมาด้วย ของที่ขาดไม่มีคนวาด

วันที่: วาดสิ่งที่โปรโตคอลทำได้และทำไม่ได้ในบริบทองค์กร · เสนอชั้นเสริม: โหวต, dissent, handoff · อัปเดตเมื่อสเปกขยับ · แพลให้กฎหมายและวิศวกรอ่านชุดเดียวกัน

ทักษะ: standards literacy · architecture · นโยบาย · การสื่อสาร

เพื่อนบ้านอาชีพ: มาจาก enterprise architect, policy technologist. ช่องว่าง: ช่องว่างระหว่างมาตรฐานเปิดกับความรับผิดชอบในบ้าน

ผู้ปรับเทียบความไว้วางใจ / Trust Calibration Designer

คนเชื่อเอเจนต์มากไปหรือน้อยไป ทั้งคู่แพง

วันที่: วัดช่องว่างระหว่างความมั่นใจของระบบกับความแม่นยำจริง · ออกแบบภาษา UI ที่ไม่ขยาด · ฝึกผู้ใช้ให้อ่านจุดที่ระบบไม่รู้ · ปรับหลังจากซ่อมแต่ละรอบ

ทักษะ: HCI · สถิติเบื้องต้น · การเขียน · field study

เพื่อนบ้านอาชีพ: มาจาก UX research, ครู, risk communication. ช่องว่าง: ช่องว่างระหว่างความรู้สึกกับความสามารถ

โปรดิวเซอร์ร่วมสร้างข้ามสัญญาณ / Trans-semiotic Co-creation Producer

เอเจนต์ศิลปะ/ดนตรี/ภาษาพัฒนากรร่วมกันจนคนตามไม่ทัน และไม่มีผู้รับผิดชอบผลงาน

วันที่: ตั้งกติกาไวยากรณ์ร่วม · กำหนดจุดที่คนลงชื่อในผลงาน · เก็บที่มาของท่อนที่เครื่องสร้าง · เจจาสัททวิและเครดิต

ทักษะ: TSCP / ศิลปะ · ลิขสิทธิ์พื้นฐาน · orchestration · การผลิต

เพื่อนบ้านอาชีพ: มาจากโปรดิวเซอร์, บรรณาธิการศิลป์, นักกฎหมายสื่อ. ช่องว่าง: ช่องว่างระหว่างการร่วมสร้างกับเครดิต

06

เล็บแปดสัปดาห์

สัปดาห์ 1: ฟังวงที่มีอยู่

3–4 ชั่วโมง · ผลลัพธ์: แผนที่ระบบหนึ่งหน้าของงานที่คุณแตะได้จริง

1. เลือกงานซ้ำหนึ่งอย่างที่คุณทำหรือเห็นทุกสัปดาห์
2. เขียน: ใครเริ่ม ข้อมูลอยู่ที่ไหน สิทธิใครถือ ผลไปไหน ความผิดพลาดเคยเกิดแบบไหน
3. วงส่วนที่คนทำ / เครื่องทำได้ / ยังห้ามเครื่องทำ
4. อย่าเปิดเฟรมเวิร์กในเล็บนี้

โหมดลัมเบิล: เริ่มที่เครื่องมือก่อนใจ — ถ้าเกิด ให้ฉีกแผ่นแล้วเริ่มใหม่ทั้งงาน

สัปดาห์ 2: เอเจนต์เดี่ยวมีขอบเขต

5–8 ชั่วโมง · ผลลัพธ์: เอเจนต์หนึ่งตัวที่ดึงความรู้เฉพาะได้และปฏิเสธของนอกเขต

1. คัดเอกสาร 5–10 ชิ้นที่คุณมีสิทธิ์ใช้
2. ตั้งข้อห้ามสามข้อในระบบ
3. ทดสอบด้วยคำถามในเขตและนอกเขต
4. จด mismatch ทุกข้อ

โหมดลัมเบิล: ปล่อยให้ตอบนอกเขตเพราะ ‘มีประโยชน์’ — นับเป็นศูนย์

สัปดาห์ 3–4: วงสามตัวกับจุดหยุดหนึ่งจุด

สองสัปดาห์แบบไม่เต็มเวลา · ผลลัพธ์: กราฟหรือครุขนาดเล็กที่มีเกตคนก่อนผลที่ย้อนกลับไม่ได้

1. แยกเป็นผู้เก็บ ผู้ร่าง ผู้ตรวจ
2. ประกาศเจตนาก่อนลงมือ
3. ใส่ interrupt ก่อนส่งออกภายนอก
4. รับสับเคส วัดคนแก้ที่ครั้ง ต้นทุนเท่าไร

โหมดลัมเบิล: เพิ่มตัวที่สี่เพราะตื่นเต้น — ห้ามจนกว่าสับเคสจะจบ

สัปดาห์ 5: ซ้อมถอดปลั๊ก

2 ชั่วโมง · ผลลัพธ์: สวิตช์ที่ทำให้วงหยุดได้ในนาที และบันทึกการซ้อม

1. สมมติเอเจนต์เริ่มทำนอกเขต
2. ถอดสวิตช์หรือหยุดกราฟจริง ๆ
3. จับเวลาและเขียนสิ่งที่ยังวิ่งต่อ
4. แก้งานเหลือช่องโหว่ที่รับได้

โหมดลิมิเต็ด: ถอดแค่ในสไลด์ — ไม่นับ

สัปดาห์ 6: ซ้อมหนึ่งเส้นทาง

ครึ่งวัน · ผลลัพธ์: เคส mismatch → ซ้อม → ความไว้วางใจถูกปรับ ไม่ใช่แค่แพตช์

1. เลือกความพลาดที่เจ็บที่สุด
2. อธิบายว่าโมเดลในหัวคนคาดอะไร
3. แก่สัญญา ข้อมูล หรือเกต
4. เขียนประโยคใหม่ว่าวงนี้ทำได้/ยังทำไม่ได้

โหมดลิมิเต็ด: ปิดบ๊ิกแล้วไม่แตะประโยคความไว้วางใจ

สัปดาห์ 7–8: เคสศึกษาและอาชีพ

สุดสัปดาห์ · ผลลัพธ์: เอกสารหนึ่งหน้า + อาชีพที่คุณอาจตั้งจากช่องว่างที่เจอ

1. เขียนเคสตามโครง: โจทย์ วง จุดหยุด ตัวเลข สิ่งทีคนยังทำ
2. ไล่ช่องว่างห้าช่องในบทคัดค้านอาชีพ
3. ร่างวันที่ของงานหนึ่งตำแหน่ง
4. หากคนหนึ่งที่เจ็บจากช่องว่างนั้นแล้วคุย

โหมดลิมิเต็ด: ตั้งชื่อเท่าก่อนมีวันที่ของงาน

07

อภิธานและแหล่งอ้างอิง

A2A

Agent-to-Agent Protocol — มาตรฐานให้เอเจนต์ต่างระบบค้นพบและส่งงานกัน (Google → Linux Foundation)

Agency

ระดับที่ระบบลงมือในโลกได้ ไม่ใช่แค่พูด การมี agency สูงต้องมีจุดหยุดที่แข็ง

Checkpoint

จุดบันทึกสถานะของกราฟ เพื่อหยุด รอคน และทำงานต่อโดยไม่ลืม

Context engineering

วินัยจัดทุกอย่างที่โมเดลเห็นตอนอนุมาน ไม่ใช่แค่การดึงเอกสาร

Context layer / lakehouse

ชั้นเก็บความรู้เฉพาะองค์กร ความรู้เจียบ และนโยบาย ให้ดึงอย่างมีสิทธิ์

Dissent preservation

การเก็บทางที่ไม่ถูกเลือกไว้เป็นหลักฐาน ไม่ให้การสรุปกลายเป็นการลบ

ETHOS

กรอบเสนอธรรมาภิบาลเอเจนต์แบบกระจายศูนย์ด้วย DAO และสัญญาอัจฉริยะ

HITL

Human-in-the-Loop — คนอยู่ในวงตัดสินใจตอนรัน ไม่ใช่แค่ตอนออกแบบ

Handoff

การส่งงานจากเครื่องสู่คนอย่างมีบริบท ทางเลือก และผู้รับที่ชัด

Indirect prompt injection

การซ่อนคำสั่งในเนื้อหาภายนอกที่เอเจนต์ไปอ่านแล้วทำตาม

Intent declaration

การบังคับให้เอเจนต์ประกาศจะทำอะไรก่อนลงมือ เพื่อจับงานกับ

LangGraph

เฟรมเวิร์กมองเอเจนต์เป็นกราฟมีสถานะ เหมาะกับโปรดักชันและจุดหยุด

MAS

Multi-Agent System — หลายเอเจนต์ หน้าที่เฉพาะ มีออร์เคสตรา

MCP

Model Context Protocol — พอร์ตมาตรฐานเชื่อมโมเดลกับเครื่องมือและข้อมูล

MPAC

Multi-Principal Agent Coordination — ประสานเอเจนต์หลายเจ้าของด้วยเจตนาและการยกระดับ

Orchestrator

คนหรือชั้นซอฟต์แวร์ที่จัดจังหวะวง ไม่เล่นทุกเครื่องเอง

PAT

Personal Access Token — โทเคนแทนตัวตนผู้ใช้ ต้องไม่กว้างกว่าสิทธิ์ของคนนั้น

RAG

Retrieval-Augmented Generation — ดึงเอกสารมาประกอบคำตอบ เป็นเสาหนึ่งของบริบท

RBAC

Role-Based Access Control — สิทธิ์ตามบทบาท เอเจนต์ต้องรับช่วงสิทธิ์นี้ ไม่ข้าม

Repair trajectory

เส้นทางหลังความผิดพลาดที่นำไปสู่การเรียนรู้ ไม่ใช่แค่ความโล่งชั่วคราว

Sequence lock

กฎห้ามบทบาทแย่งจังหวะกัน เช่น ห้ามสอนพร้อมกัน

Stop architecture

การออกแบบจุดที่วงต้องเจียบ ส่งคน หรือถอดปลั๊ก

Tacit knowledge

ความรู้ที่ผู้เชี่ยวชาญทำได้แต่ยังไม่ได้เขียน เป็นวัตถุดิบของชั้นบริบท

TSCP

Trans-Semiotic Co-Creation Protocols — กติกาการร่วมสร้างข้ามสื่อระหว่างเอเจนต์

แกนทั้งห้าสังเคราะห์จากคลัง 67 แหล่งในระบบต้นทางของผู้ใช้ แล้วขยายด้วยแหล่งเปิดอิสระด้านบน ตัวเลขตลาดแรงงานเปลี่ยนเร็ว และควรถูกอ่านเป็นทิศทาง ไม่ใช่สัญญาจ้าง

1. Introducing the Model Context Protocol. Anthropic, 2024.

<https://www.anthropic.com/news/model-context-protocol>

ประกาศ MCP ในฐานะมาตรฐานเปิดเชื่อมโมเดลกับแหล่งข้อมูลและเครื่องมือ

2. Model Context Protocol specification. modelcontextprotocol.io, 2025–2026.

<https://modelcontextprotocol.io>

สเปกที่เป็นทางการ รวม structured output, elicitation, streamable HTTP

3. MCP donated to the Agentic AI Foundation. Linux Foundation / AAIF, 2025.

https://en.wikipedia.org/wiki/Model_Context_Protocol

การย้ายธรรมาภิบาลโปรโตคอลออกจากผู้ขายรายเดียว

4. Announcing the Agent2Agent Protocol (A2A). Google Developers Blog, 2025.

<https://developers.googleblog.com/en/a2a-a-new-era-of-agent-interoperability/>

เปิดตัว A2A พร้อมพันธมิตรตั้งต้นกว่า 50 องค์กร

5. A2A Protocol surpasses 150 organizations. Linux Foundation, 2026.

<https://www.linuxfoundation.org/press/a2a-protocol-surpasses-150-organizations-lands-in->

major-cloud-platforms-and-sees-enterprise-production-use-in-first-year

ครบหนึ่งปี: คลาวด์ใหญ่และการใช้งานโปรดักชัน

6. A2A Protocol. [a2a-protocol.org / GitHub a2aproject](https://a2a-protocol.org/latest/), 2025–2026. <https://a2a-protocol.org/latest/>
ที่อยู่สเปกปัจจุบันของโปรโตคอลเอเจนต์ต่อเอเจนต์
7. LangGraph documentation — durable execution & interrupts. LangChain, 2025–2026. <https://langchain.com>
กราฟมีสถานะ จุดหยุด และ checkpoint สำหรับ HITL
8. CrewAI / AutoGen comparisons for production MAS. industry surveys 2026, 2026. <https://www.langchain.com/resources/ai-agent-frameworks>
บทบาทต่างกัน: กราฟสำหรับโปรดักชัน ครูสำหรับต้นแบบ สกนนาสำหรับงานถก
9. OWASP Top 10 for LLM Applications. OWASP GenAI, 2025. <https://genai.owasp.org/llm-top-10/>
Prompt injection โดยเฉพาะทางอ้อม เป็นความเสี่ยงหัวตารางของเอเจนต์
10. LLM01: Prompt Injection. OWASP, 2025. <https://genai.owasp.org/llmrisk/llm01-prompt-injection/>
นิยาม indirect injection จากหน้าเว็บ ไฟล์ และแหล่งภายนอก
11. Decentralized Governance of AI Agents (ETHOS). Chaffer et al., arXiv:2412.17114, 2025. <https://arxiv.org/html/2412.17114v3>
กรอบใช้ DAO / blockchain สำหรับทะเบียนและกำกับเอเจนต์
12. Future of Jobs Report 2025. World Economic Forum, 2025. <https://www.weforum.org/publications/the-future-of-jobs-report-2025/>
ทักษะ AI และบิกดาต้าโตเร็วสุด นายจ้างกว่า 1,000 ราย
13. Invest in the workforce for the AI age. World Economic Forum, 2026. <https://www.weforum.org/stories/artificial-intelligence/ai-roadmap-transforming/>
ผลผลิตมาจากการจัดวงคน-เครื่อง ไม่ใช่การแทนที่เปล่า ๆ
14. The most important job of 2026? AI agent orchestration. Eightfold, 2025. <https://eightfold.ai/blog/most-important-job-2026/>
นิยามสมรรถนะ: ระบบ กระบวนการ โดเมน การเปลี่ยนแปลง ธรรมชาติ
15. AI orchestration compensation snapshots. ZipRecruiter market pulldown, 2026. <https://www.ziprecruiter.com/Jobs/Ai-Orchestration>
สัญญาณตลาดสหรัฐ ไม่ใช่ค่าจ้างสากล — ใช้เทียบทิศทาง
16. Context Engineering vs RAG. Atlan / DataHub / Sourcegraph analyses, 2026. <https://sourcegraph.com/blog/context-engineering>
RAG เป็นเสาหนึ่งของบริบท ไม่ใช่ทั้งสถาปัตยกรรม

7. Write, Select, Compress, Isolate. LangChain context engineering framing, 2025–2026.
<https://karozieminski.substack.com/p/context-engineering-product-builders-guide-2026>
 สักลยกรพื้นฐานที่วากยกรใช้จัดหน้าต่างบริบท
8. Human-in-the-loop interrupts and approval hubs. LangGraph community / CopilotKit, 2026.
<https://www.openlegion.ai/en/learn/human-in-the-loop-ai-agents>
 แยกเขตที่กราฟบังคับกับคำถามที่โมเดลเลือกจะถาม
9. Agent-to-agent communication landscape (A2A, MCP, ACP, ANP). industry research notes, 2026. <https://zylos.ai/research/2026-02-15-agent-to-agent-communication-protocols/>
 แผนที่โปรโตคอลที่เสริมกัน ไม่ใช่สนามรบศูนย์รวม
10. Skills required for building AI agents in 2026. practitioner essays, 2026.
<https://dev.to/imaginex/skills-required-for-building-ai-agents-in-2026-2ed>
 orchestration และ problem shaping แสงการเขียนโค้ดจากศูนย์ในฐานะตัวแบ่ง

08

บทส่งท้าย

ถ้าอ่านจบแล้วยังไม่ได้เลือกงานชิ้นหนึ่งในชีวิตจริง เอกสารนี้ยังไม่เริ่มทำงาน

กลับไปเลียบที่ 1 วาดแผนที่ระบบ แล้วขึ้นแท่นวาทกยกรเลิกภายในเก้าสิบวัน

เมื่อเจอช่องว่างที่เกิดซ้ำ อย่ารอให้ HR ตั้งชื่อ ให้คุณตั้งอาชีพ แล้วพิสูจน์ด้วยวันที่ของงาน

เครื่องมือที่หยุดไม่ได้ ไม่ใช่เครื่องมืออีกต่อไป