

Getting Agents to Give Up Their Secrets

A guide to AI that actually works

**Last month, someone spent 45 minutes
on a one-page summary using ChatGPT.
The right approach took 2 minutes.**

This deck is
about
the trick.





Most people are here. This deck takes you here.

1 billion+

use AI tools monthly

< 2%

pay for premium

PCs

1980s

Internet

1990s

Smartphones

2010s

AI

Now



\$4.4T

in annual value. Only 31% in full production.

The core skill for AI
is talking.

You already have it.

Let's see what most people get wrong.

ChatGPT
deep
learning
OpenAI

Gemini

copilot
parameters

API

GPT

transformer
agents

tokens

fine-tuning

inference
embeddings

hallucination

AGI
context
window

LLM

neural net

training
Claude

MCP

RAG

vector DB
prompts

Anthropic

open-source
grounding

GPT

What's the difference
between ChatGPT and
GPT?

Gemini

What even is
an agent?

copilot

LLM

tokens

AGI

Claude

Is Claude the same
as ChatGPT?

training

Do I need to know
what a token is?

App

Agent

API

LLM

You use apps.
Apps use agents.
Agents call APIs.
APIs talk to LLMs.

Who Makes What

Company	LLM	App
OpenAI	GPT	ChatGPT
Anthropic	Claude	Claude.ai
Google	Gemini	Gemini
Microsoft	(OpenAI's)	Copilot

The real action is in
agents and apps.

41%

of GitHub code is now AI-generated

19%

longer

when developers rely on AI
without understanding it

The gap between using
AI
and using AI well
is massive.

10×

Microsoft 365 Copilot daily users,
year over year

*You've got the basics.
Now let's give you the skills.*

Prompt Engineering

How to Stop Getting Useless Answers

Write me a proposal for improving
our onboarding process.

→ Generic, surface-level output

Assign a Role

vs. talking to a stranger

Write me a proposal for improving our onboarding process.

You are a senior HR operations consultant. Write me a proposal for improving our onboarding process.

Be Specific

vs. the vague ask

Write me a proposal for improving our onboarding process.

Write a proposal for reducing onboarding from 4 to 2 weeks, for the VP of People, under 2 pages.

One Task at a Time

vs. the kitchen sink

Write the proposal, draft an email, create a budget spreadsheet, and summarize risks.

Structure the proposal with:

1. Problem statement
2. Proposed solution
3. Expected outcomes
4. Timeline

Power Keywords

vs. leading the witness

Don't you think reducing
onboarding to 2 weeks
would be great?

Be radically honest about
challenges.
Think step by step.
Challenge my assumptions.

Define the Output

vs. hoping for the best

(No format guidance)
→ Random format, 5-page
essay
when you needed bullets.

One-page executive brief
with
bullet points. Data-driven
language.
Reader has 2 minutes.

Before

"Write me a proposal for improving our onboarding process."

After

Senior HR consultant
4 to 2 weeks, VP of People
Step by step, challenge
me
One-page brief, bullets

**Same task. Same
information.
Just better words.**

**But we never changed
what the AI knew.**

*You've changed the words.
Now let's change the information.*

**Same prompt.
Different information.**

Dramatically different result.

**Plausible but
generic**

Could be for any company.

**Sounds like
someone
who works here**

Same prompt + your context.



Meet your
AI colleague.

Brilliant. Helpful.
Remembers
nothing.

Too much.
Contradictory.
Too broad.

Three ways to confuse your AI.

**Let AI tell you
what it needs.**

"Before you start, ask me clarifying
questions."

**Not too much.
Not too little.**

The right context at the right time.

**You've mastered context.
But you're providing it
from scratch every time.**

Directions every trip

Effort. Every. Time.

GPS that learns

Compounds permanently.

"Custom instructions"

= "System prompts"

= "Rules"

= "Skills"

*You talk to AI like a pro.
You've set up its playbook.
But who's doing all the work? Still you.*

1. You search

2. You paste

3. AI drafts

4. You apply

You're using a Ferrari
to carry groceries.

1. Agent retrieves

2. Agent identifies gaps

3. Agent creates

4. You review

**Same colleague.
Now she has hands.**

Eyes, a phone, and a to-do list.



Web



Email



Docs



Data



Calendar



Custom

Without

You copy-paste
You forget the budget memo
VP asks — too late

With

Agent reads directly
Finds what you forgot
Flags what you missed

Trust, but verify.

Never trust numbers you didn't provide.

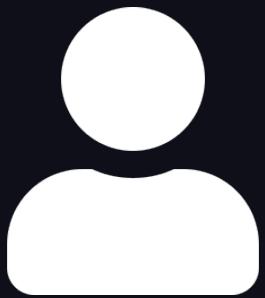
Verify claims against sources.

Use AI for drafts, not decisions.

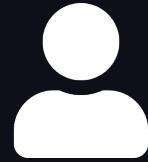
**AI is a power tool,
not autopilot.**

**When the answer ‘feels right’
but you can’t verify it —
that’s the most dangerous
moment.**

*You're managing AI well.
Time to orchestrate it.*



One Chef



Prep



Grill



Sauce



Plate

**The trick isn't making
one AI smarter.
It's making many
work together.**

Research



Draft



Review



You

**Each agent does one
thing.**

**The chain does
everything.**

Skills

You already know these.
Now each agent gets its own.

Research Agent

+ Research
Standards

Draft Agent

+ Leadership
Proposals

Review Agent

+ Compliance Policy

**Skills compound.
The brigade gets smarter
every time.**

1.5 hrs

of you being the bottleneck

15 min

of judgment — the part only humans can do

**Same proposal.
The chain gets smarter
every time.**

Your feedback becomes skills. She won't
remember, but the skills will.

Let's come back to where we started.

**Remember the
45-minute summary?**

Two minutes.
That's the
trick.

**The secret was never
in the AI.**

Now go try it — one task, this week.