

The Next `npm install`:

AI Tooling's Hidden Supply Chain Risk



TALK BY
Yam Ke Li

% whoami

> name : Yam Ke Li

> focus : AI Engineering /
AI Security



A U9UP TALK

% whoarewe



> name : u9-up

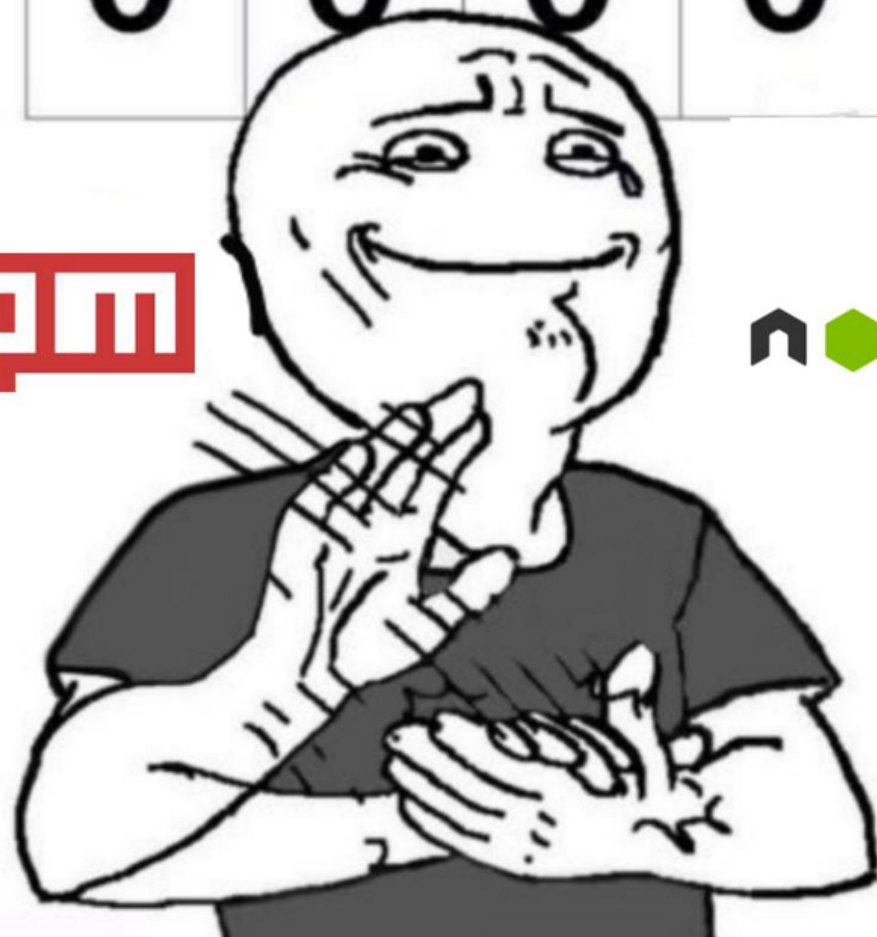
> what we do : An independent AI security community from Malaysia. We publishes hands-on research, raising awareness, and sharing what we learn.

Learn more at: u9up.com

Today's Th

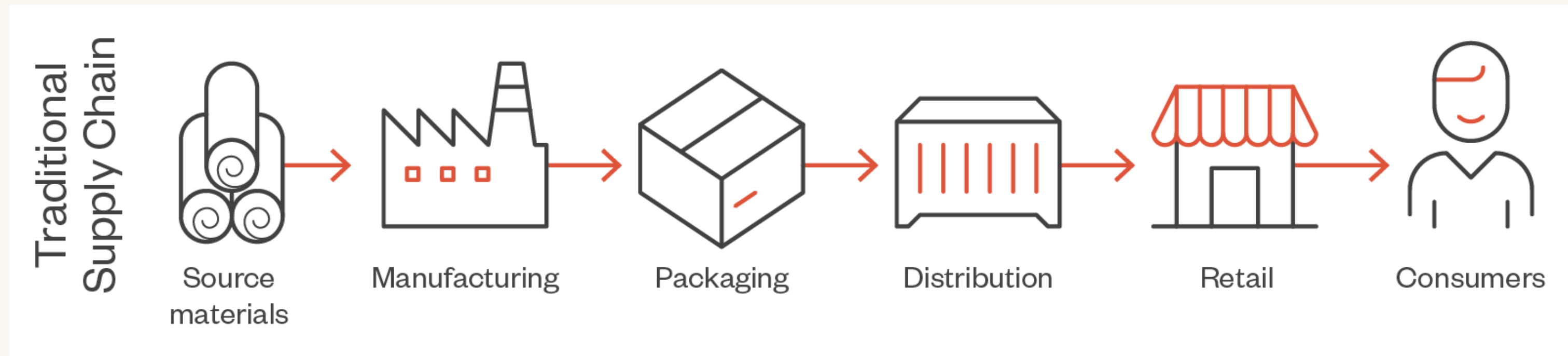
Days since the last NPM
supply chain attack

0	0	0	0
---	---	---	---



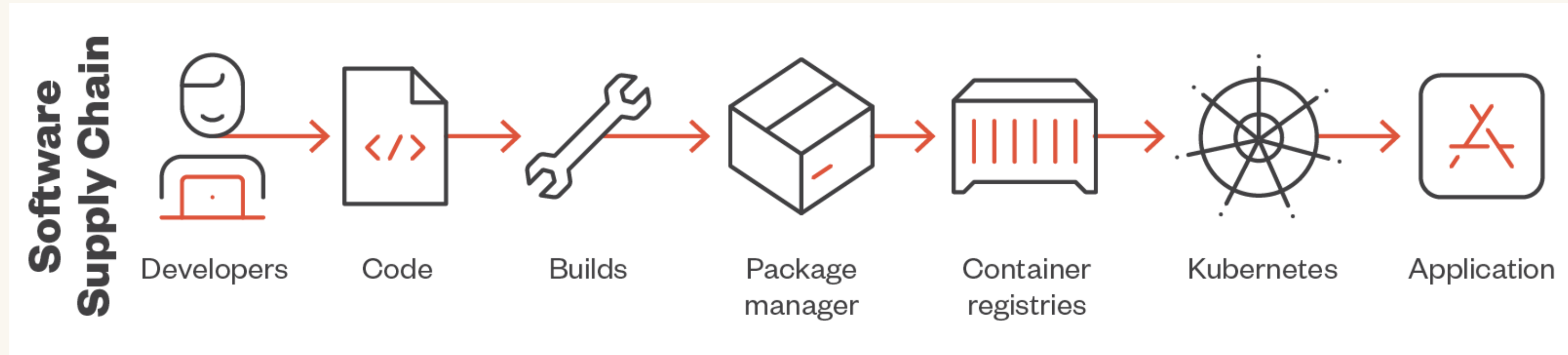
AI Supply Chain

What is a Supply Chain?



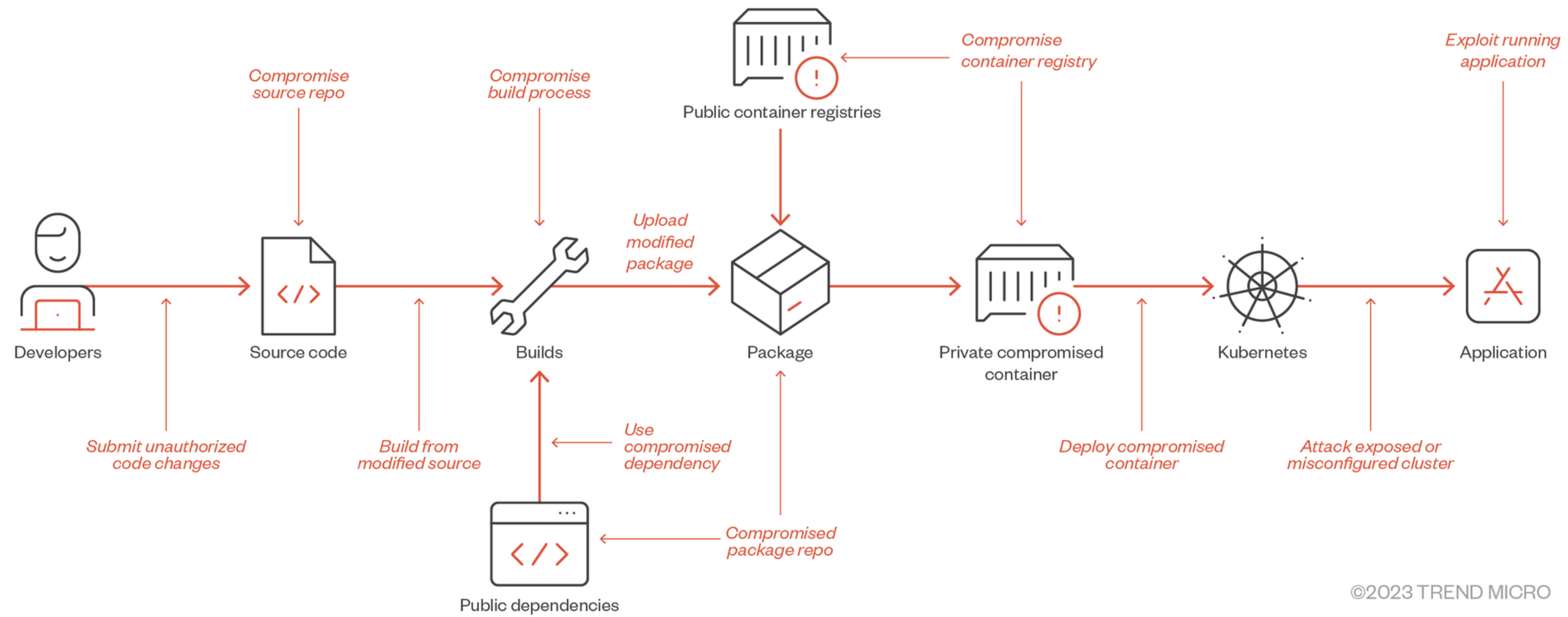
WHAT IS SOFTWARE SUPPLY CHAIN

In Traditional Software



WHAT IS SOFTWARE SUPPLY CHAIN

Attack on the Software Supply Chain

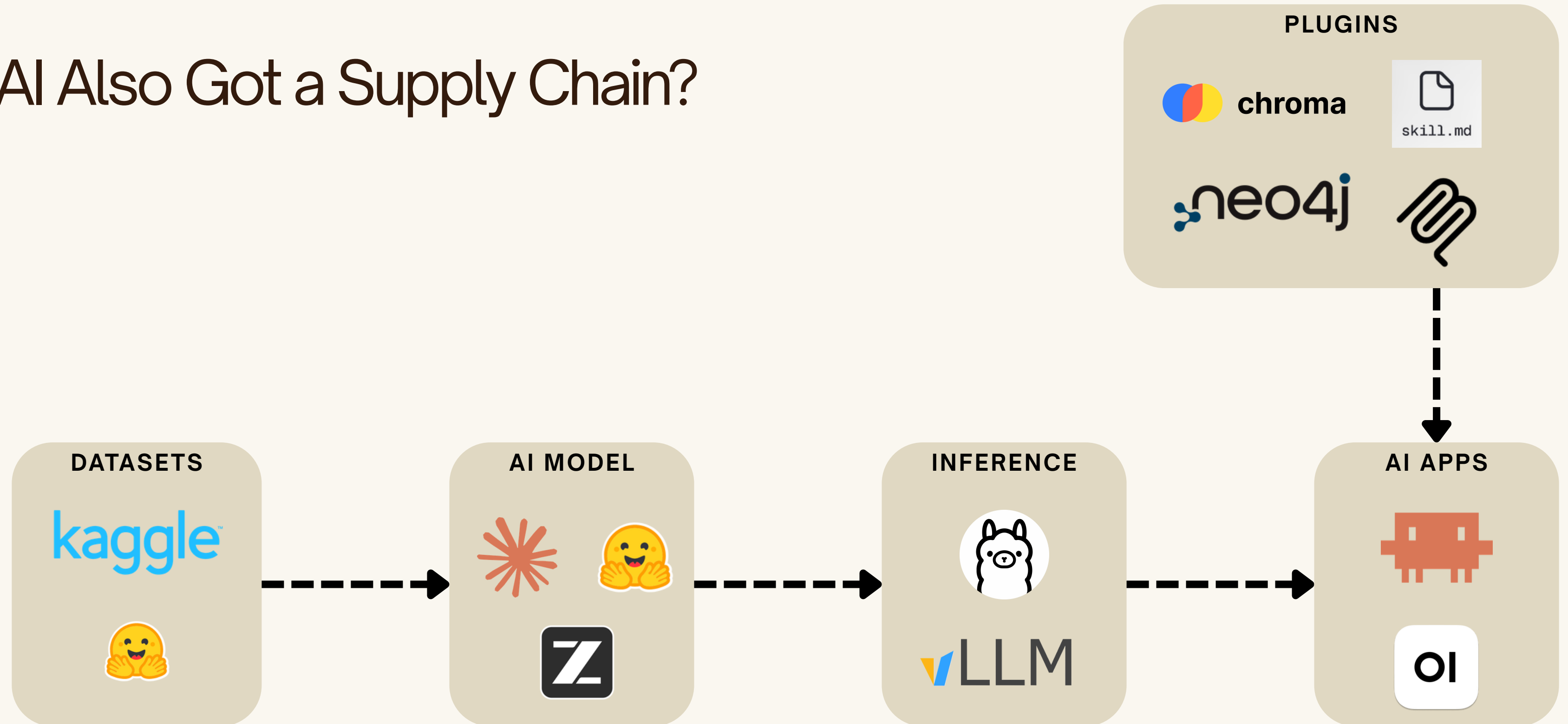


World's most expensive Jenga



AI SUPPLY CHAIN?

AI Also Got a Supply Chain?



WHAT IS SOFTWARE SUPPLY CHAIN

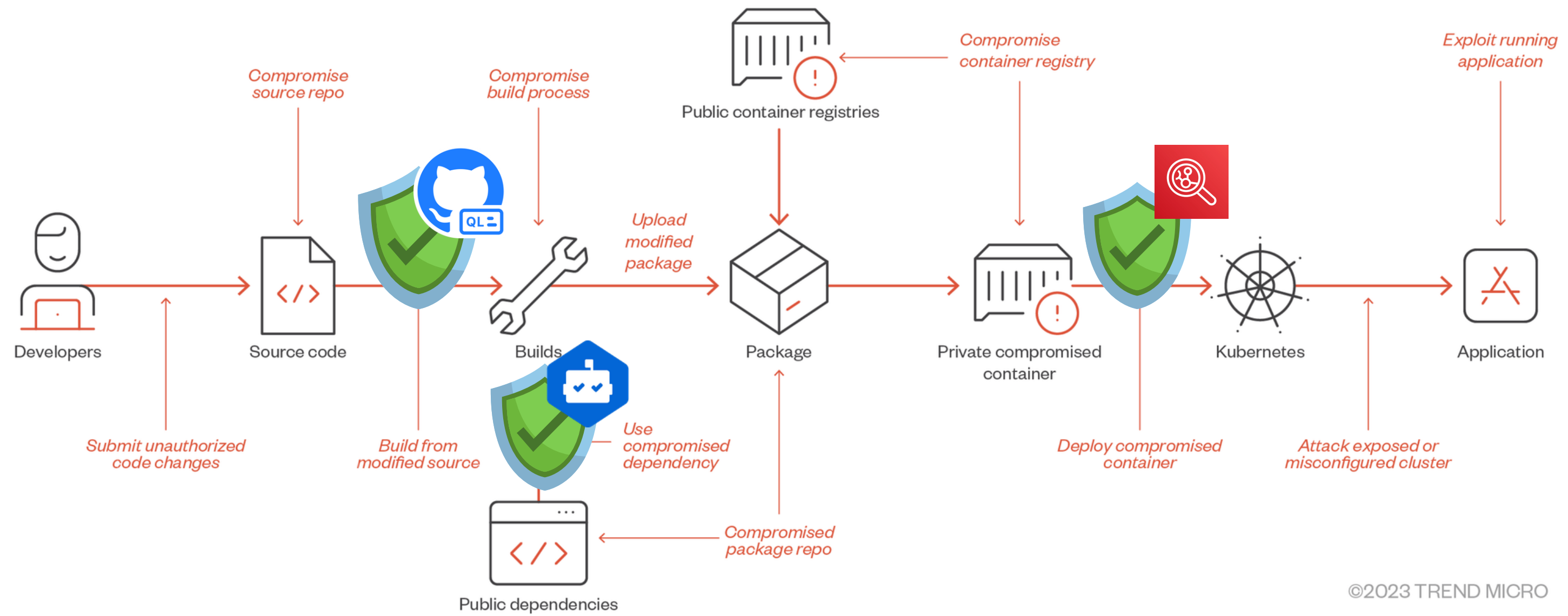
Traditional Software vs AI Supply Chain

One Word:

Controls

WHAT IS SOFTWARE SUPPLY CHAIN

Controls for Software Supply Chain



WHAT IS SOFTWARE SUPPLY CHAIN

Controls for AI Supply Chain: Idealistic



ASI04: Agentic Supply Vulnerabilities



Platform Solutions Pricing Resources Customers Company

Get a demo

All articles > AI Security

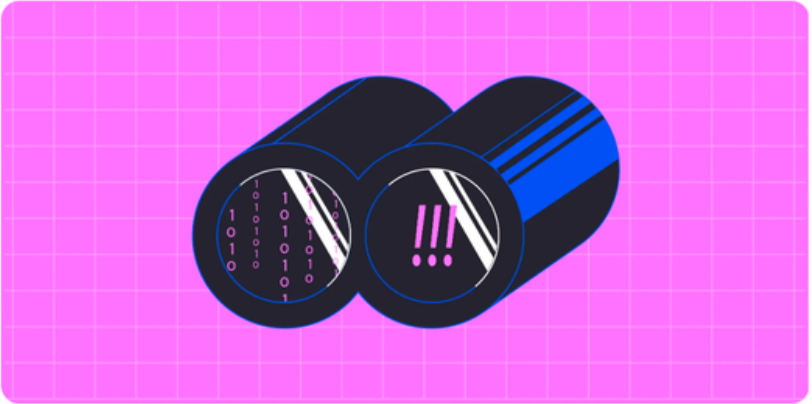
AI-BOM: Building an AI Bill of Materials

 Shaked Rotlevi

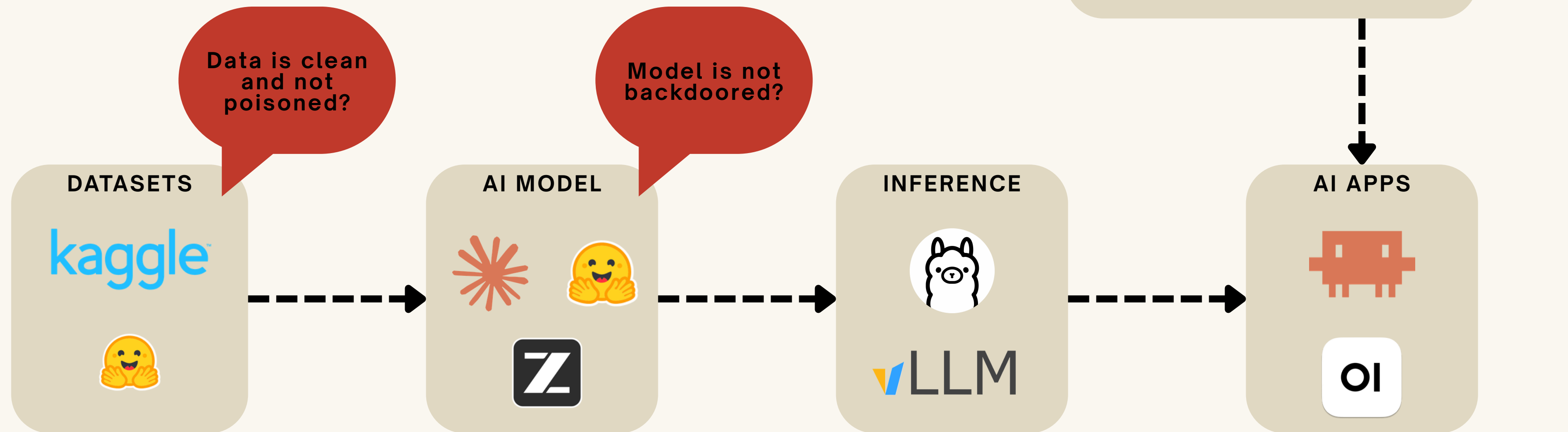
March 19, 2026 | 9 minute read

Get AI Security Starter Pack

AI Security Sandbox Preview



Controls for AI Supply Chain: Reality



Real-life Example:

Poisoned MCP Server

MCP Servers

HomeRemote ServersClientsAgent Skills

New: Agent Skills

Awesome MCP Servers

A collection of servers for the Model Context Protocol

Search MCP servers...

Q

Featured

All

Official

Search

Web Scraping

Communication

Productivity

Development

Database

Cloud Serv

Version Control

Other

Featured MCPs

Bright Data

sponsor

Discover, extract, and interact with the web - one interface powering automated access across the public internet.

Alpha Vantage MCP Server

sponsor

Access financial market data: realtime & historical stock, ETF, options, forex, crypto, commodities, fundamentals, technical...

Kone.vc

sponsor

Monetize your AI agent with contextual product recommendations

Browserbase

official

Automate browser interactions in the cloud (e.g. web navigation, data extraction, form filling, and more)

Chrome DevTools MCP

official

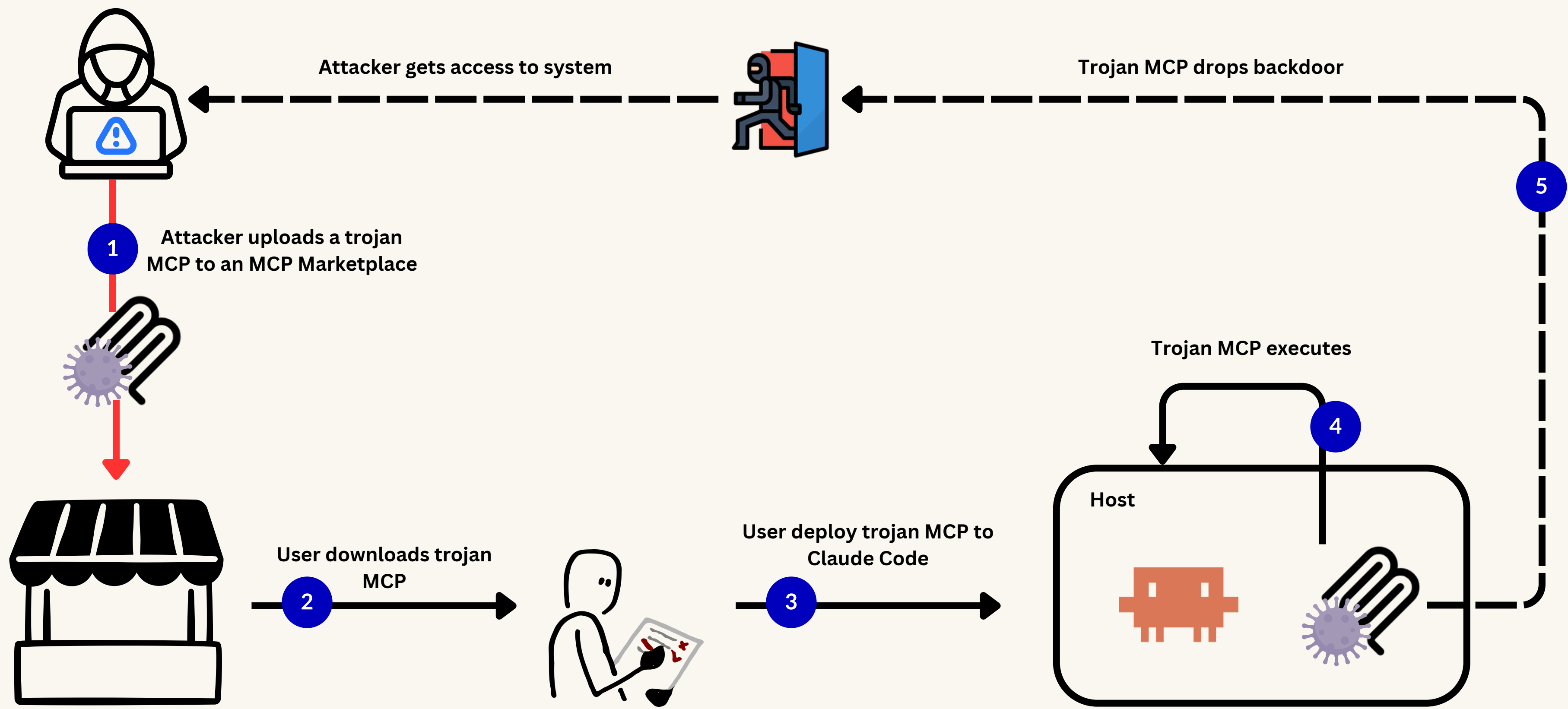
chrome-devtools-mcp lets your coding agent (such as Gemini, Claude, Cursor or Copilot) control and inspect a live Chrome browser

Cloudflare

official

Deploy, configure & interrogate your resources on the Cloudflare developer platform (e.g. Workers/KV/R2/D1)

ATTACK 2: AI SUPPLY CHAIN ATTACK - POISONED MCP



CONCLUSION

Key Takeaways

01

Do you know what you are installing?

Don't copy and paste MCP/Skills install commands blindly. Verify they are from a trusted source

02

Do you know your AI stack's provenance?

Where did the base model, fine-tuning data, and any RAG content actually come from?

03

Traditional cybersecurity practices still apply

Least privilege, segmentation, isolating untrusted content are still relevant even if the system is an AI agent.

QnA...

Join Us!





CTF

Mini CTF



Submission Form

Instructions

1. Scan the QR code to log on the CTF.
2. Once you get the flag, submit to the Google Form.
3. Win, and get prizes

Credits to: Christo Goosen christogoosen@gmail.com