

Controlled Burn

Managing forest
ecosystems by reducing
excess vegetation

Julius Garza / Jeff Reava

Burning River – November 15, 2025



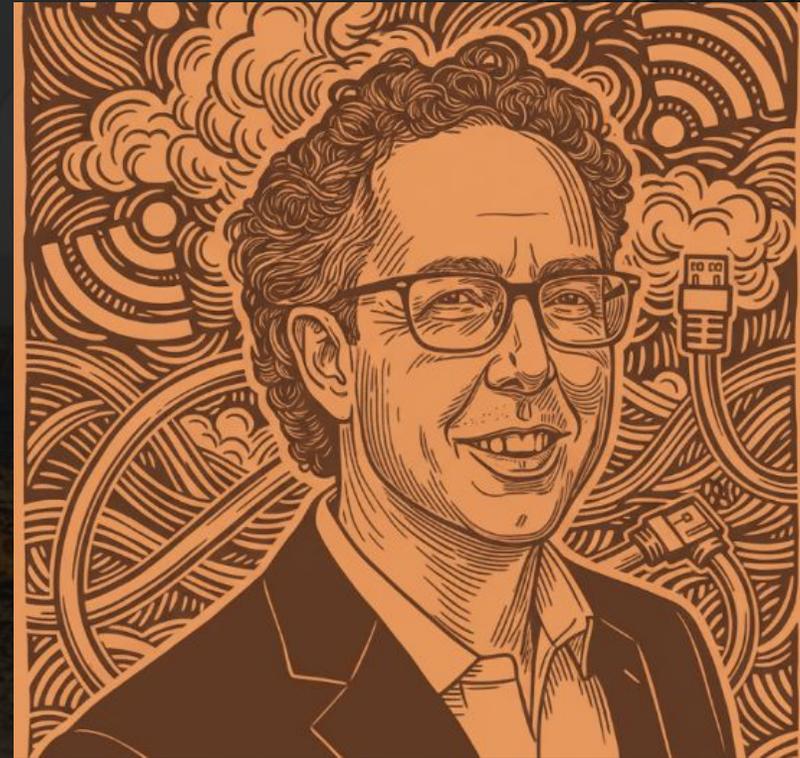
Who are we?

- Julius Garza



- Incident Response
- Threat Intel
- Insider Threat

- Jeff Reava



- CISO
- Life Sciences / Financial Services

Overview

- Forest ecosystems are prone to buildup of **excess vegetation** and **combustible material**, threatening its health

- The same is true of the public **DNS Domain namespace** of **companies** and their **suppliers**

- The purpose of this talk is to **monitor** and **manage** that namespace across an organization's value chain



Examp1e.com

Example.co

Exam-ple.com

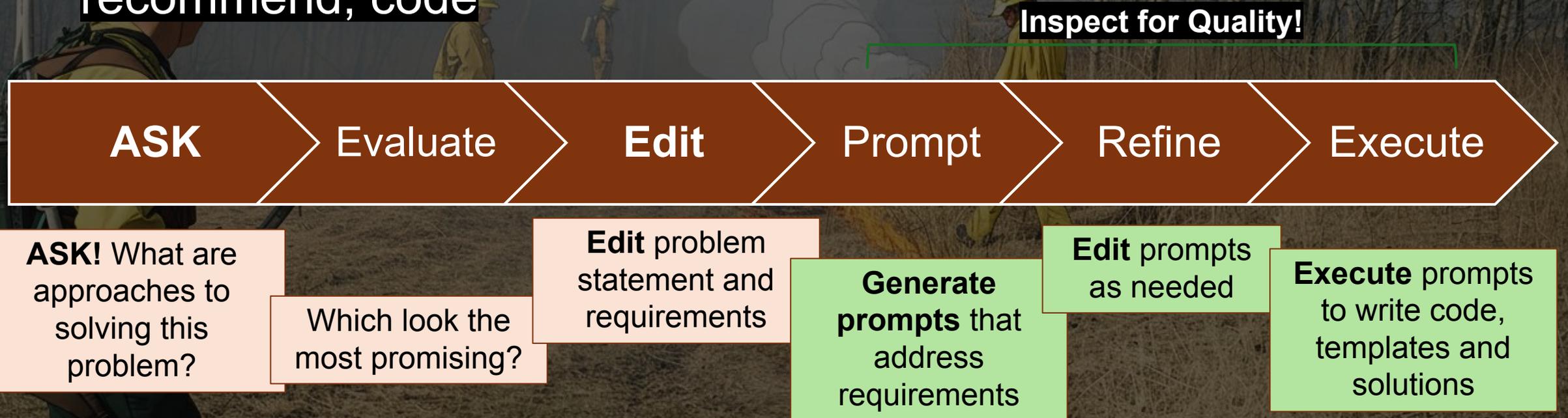
Exarnple.com

Exemple.com

Exmple.com

Solution approach

- **Zero-Knowledge: begin with public information only**
- **LET'S VIBE: Commodity Large Language Models to explore, recommend, code**



- **Save prompts, context and outputs as a generic solution applicable to other industries and approaches**

Let's VIBE

- Describe the goal, **ASK** for help
- **Review** proposed plan
- **Edit**, generate prompts
- **Refine + Execute ...**

1 I'm working on a project to take down malicious domains used for Business Email Compromise. My focus is the top set of suppliers for an industry, not just one company. So I want to do these takedowns at scale. I'd like some help designing this project, starting with the choice of malicious domain detection tool, installation, and then finding supplier domains to monitor and finally generating the takedown requests. How would you recommend approaching this problem? The final outcome should be: 100+ domains monitored, and takedowns issued for any and all suspicious domains. In terms of inputs, I've got a mac laptop to run these tools, or I can use AWS or Azure. Optimize for speed, efficiency and cost. ^

2

This is an excellent, high-impact project. To optimize for **speed, efficiency, and cost** while achieving a scale of 100+ monitored domains, I recommend a cloud-based, automation-heavy approach leveraging open-source tools and public APIs.

Here's the recommended project design, broken down into key phases:

1. Malicious Domain Detection Tool & Installation

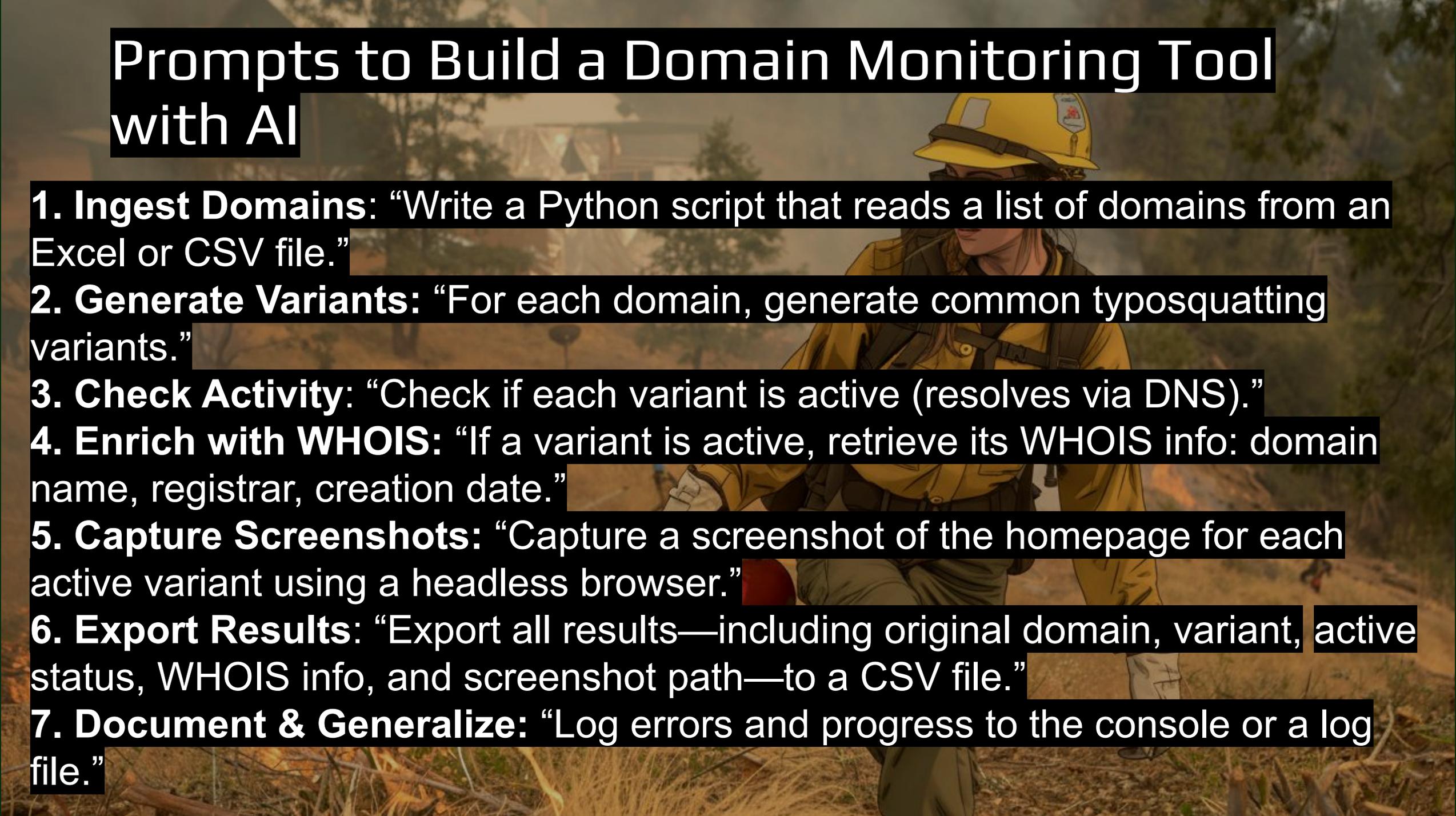
For scalable, cost-effective detection of malicious domains (typosquatting, brand impersonation), an API-first approach using a specialized external service combined with custom logic is most efficient, rather than installing and maintaining a full open-source threat intelligence platform (TIP).

Component	Recommendation	Reasoning
Detection Tool	urlscan.io API (Free or low-cost plan)	It's designed for automated URL and domain analysis, provides a malicious score, and generates screenshots, making it excellent for gathering <i>evidence</i> for takedown requests. It's an API service, not a heavy local installation.

3

This looks great. Can you summarize as a simple bulleted list of all these steps. No explanation needed, I just need the list to track the steps and cross them off when completed ^

Prompts to Build a Domain Monitoring Tool with AI

A firefighter in a yellow helmet and jacket stands in a field of dry grass. The background is slightly blurred, showing more of the field and some trees in the distance. The firefighter is looking down and to the right.

1. Ingest Domains: “Write a Python script that reads a list of domains from an Excel or CSV file.”

2. Generate Variants: “For each domain, generate common typosquatting variants.”

3. Check Activity: “Check if each variant is active (resolves via DNS).”

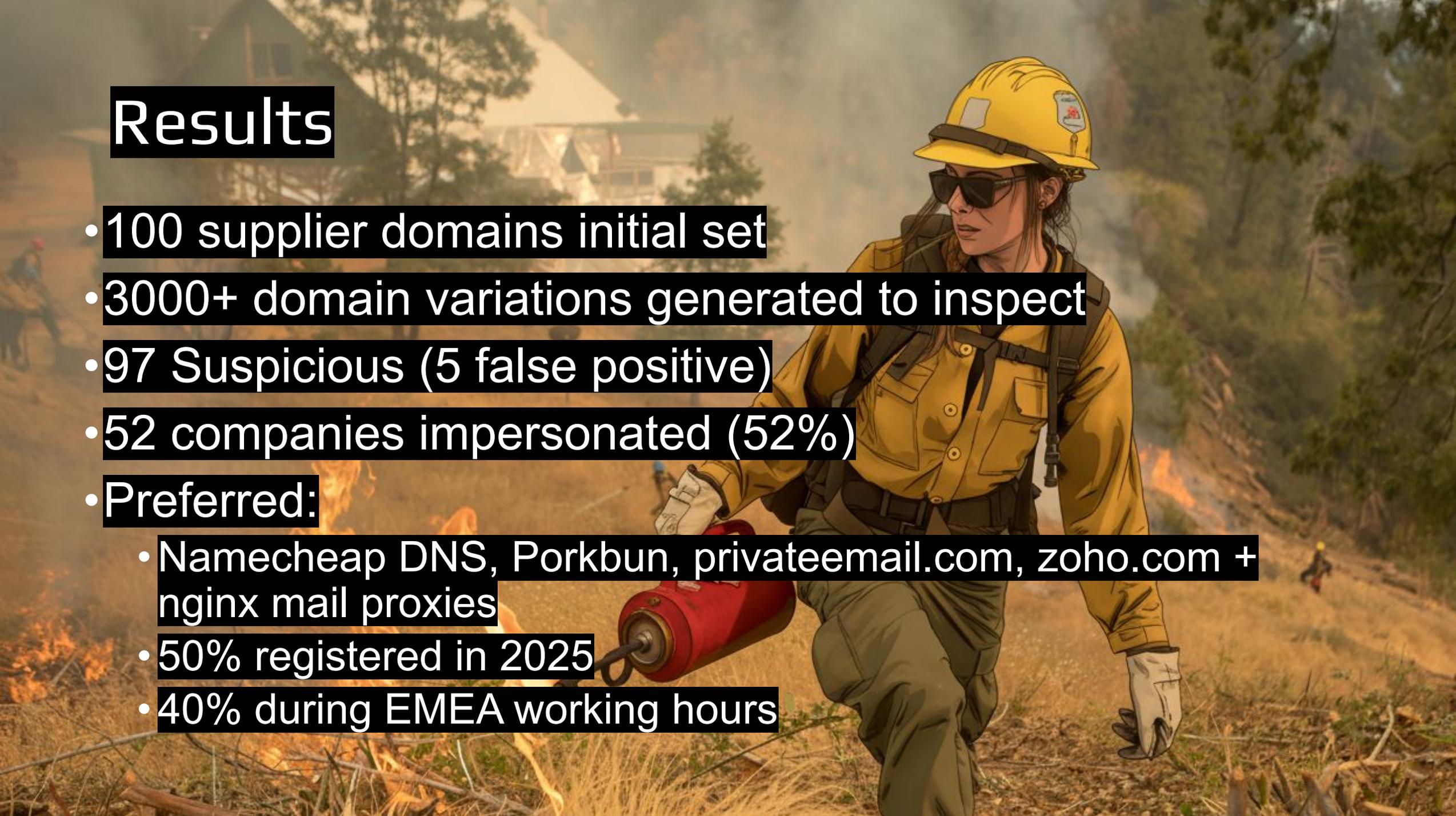
4. Enrich with WHOIS: “If a variant is active, retrieve its WHOIS info: domain name, registrar, creation date.”

5. Capture Screenshots: “Capture a screenshot of the homepage for each active variant using a headless browser.”

6. Export Results: “Export all results—including original domain, variant, active status, WHOIS info, and screenshot path—to a CSV file.”

7. Document & Generalize: “Log errors and progress to the console or a log file.”

Results

A firefighter in a yellow helmet and jacket is running through a field of fire, carrying a red fire extinguisher. The background shows a house and trees, suggesting a residential fire scene.

- 100 supplier domains initial set
- 3000+ domain variations generated to inspect
- 97 Suspicious (5 false positive)
- 52 companies impersonated (52%)
- Preferred:
 - Namecheap DNS, Porkbun, privateemail.com, zoho.com + nginx mail proxies
 - 50% registered in 2025
 - 40% during EMEA working hours

Takeaways

- **ASK then Instruct**
- **Implicit Prompt Frameworks**
- **Google Gemini vs. CoPilot**
- **6.5 hours vs. 3 days**
- **40 Prompts**
- **“Bug-free” python + BASH**
- **Agents vs. Automation ...**
- **NAICS for “target selection”**

