
ROOTCON 20 · CLARK · SEPTEMBER 2026

From Dusk Till Dawn

How Hacking & The Community Has Shifted, Pivoted, and Come Full Circle

Dhillon "@L33tdawg" Kannabhiran
Founder, Hack In The Box

2002

**The first conference
had someone else's
name on it**



DECEMBER 2003

What a hacker conference looked like then



ROOTCON 20

Twenty years of neutral ground



THE ETHIC

The hacker ethic



1986 TO 2012

The word becomes a job title



2012 ONWARD

Bug hunting becomes a market



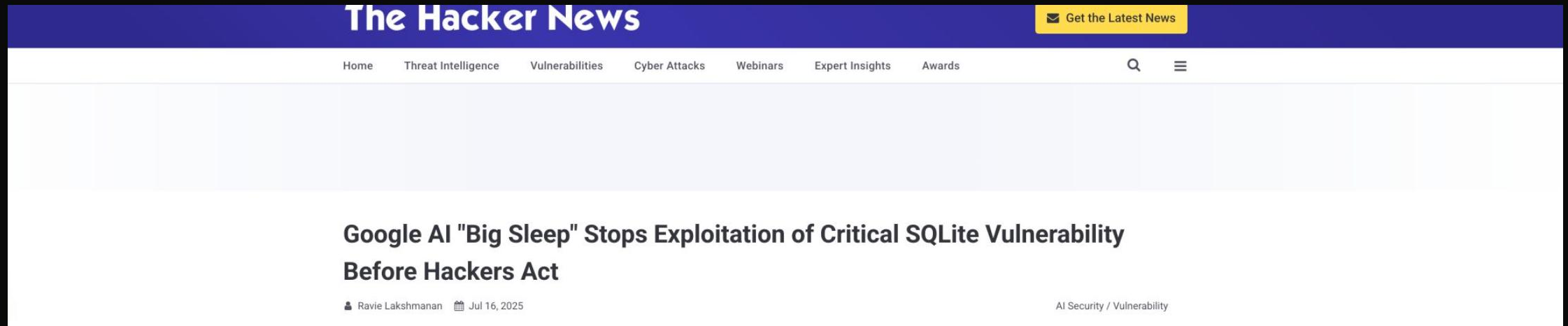


OCTOBER 2024

A machine found something nobody had found

OCTOBER 2024

The SQLite result, and why it matters



Big Sleep is a joint project between Google Project Zero and DeepMind. It found an exploitable stack buffer underflow in SQLite. The project's own fuzzing and the OSS-Fuzz infrastructure had both walked past it. Project Zero called it the first public example of an AI agent finding a previously unknown exploitable memory safety issue in widely used software.

Source: The Hacker News, 16 July 2025

NOVEMBER 2024

The write-up that changed the argument



Team Atlanta had found a null pointer dereference in SQLite at DARPA's competition, and that is what sent Big Sleep looking at the same file. Within a year the same system had found twenty more vulnerabilities in open source projects. Agents were already handing each other leads.

Source: Google Project Zero

JUNE 2025

The leaderboard stopped being human only

#1

HackerOne

First autonomous system to rank #1.
(June 2025)

1st

Autonomous System

Ranked on Microsoft's MSRC leaderboard.

14,000_±

Zero Days

Found in real customer applications.

XBOW became the first autonomous system to rank first on HackerOne, competing head to head against human researchers for a full season. It later ranked first on Microsoft's MSRC leaderboard. The company says its engine has turned up more than fourteen thousand zero days in customer applications.

MARCH 2026

An agentic security researcher shipped as a product

October 30, 2025 Security Product Research Release

Introducing Aardvark: OpenAI's agentic security researcher

Now in private beta: an AI agent that thinks like a security researcher and scales to meet the demands of modern software.

OpenAI announced Aardvark in October 2025 and folded it into Codex four months later. On reference repositories it identified ninety two percent of known and injected vulnerabilities. It reads commits, proves exploitability in a sandbox, then hands over a patch for a human to approve.

Source: openai.com

MAY 2026

Microsoft rebuilt bug hunting around agents

May 12 · 16 min read

Defense at AI speed: Microsoft's new multi-model agentic security system tops leading industry benchmark

By [Taesoo Kim](#), Vice President, Agentic Security, Microsoft



MDASH runs a panel of specialised agents across frontier and distilled models, with a second group arguing the findings down before anything is reported. It surfaced sixteen new CVEs in the Windows networking and authentication stack, four of them critical remote code execution, and topped the CyberGym benchmark of fifteen hundred and seven real world vulnerabilities.

Source: Microsoft Security



WHAT ACTUALLY CHANGED

Nothing here needed a bigger team

THE HONEST PART

**Finding is cheap
now. Deciding is
not.**



THE NEW SURFACE

Agents are where the bugs live now



MARCH 2026

One in eight AI breaches is now agentic

NEWSROOM

HiddenLayer Releases the 2026 AI Threat Landscape Report, Spotlighting the Rise of Agentic AI and the Expanding Attack Surface of Autonomous Systems

HiddenLayer surveyed two hundred and fifty security leaders. Thirty five percent traced AI breaches back to malware hidden in public model and code repositories. Seventy six percent now call shadow AI a definite or probable problem, up from sixty one percent the year before. Thirty one percent do not know whether they were breached at all.

Source: HiddenLayer

THE JOBS QUESTION

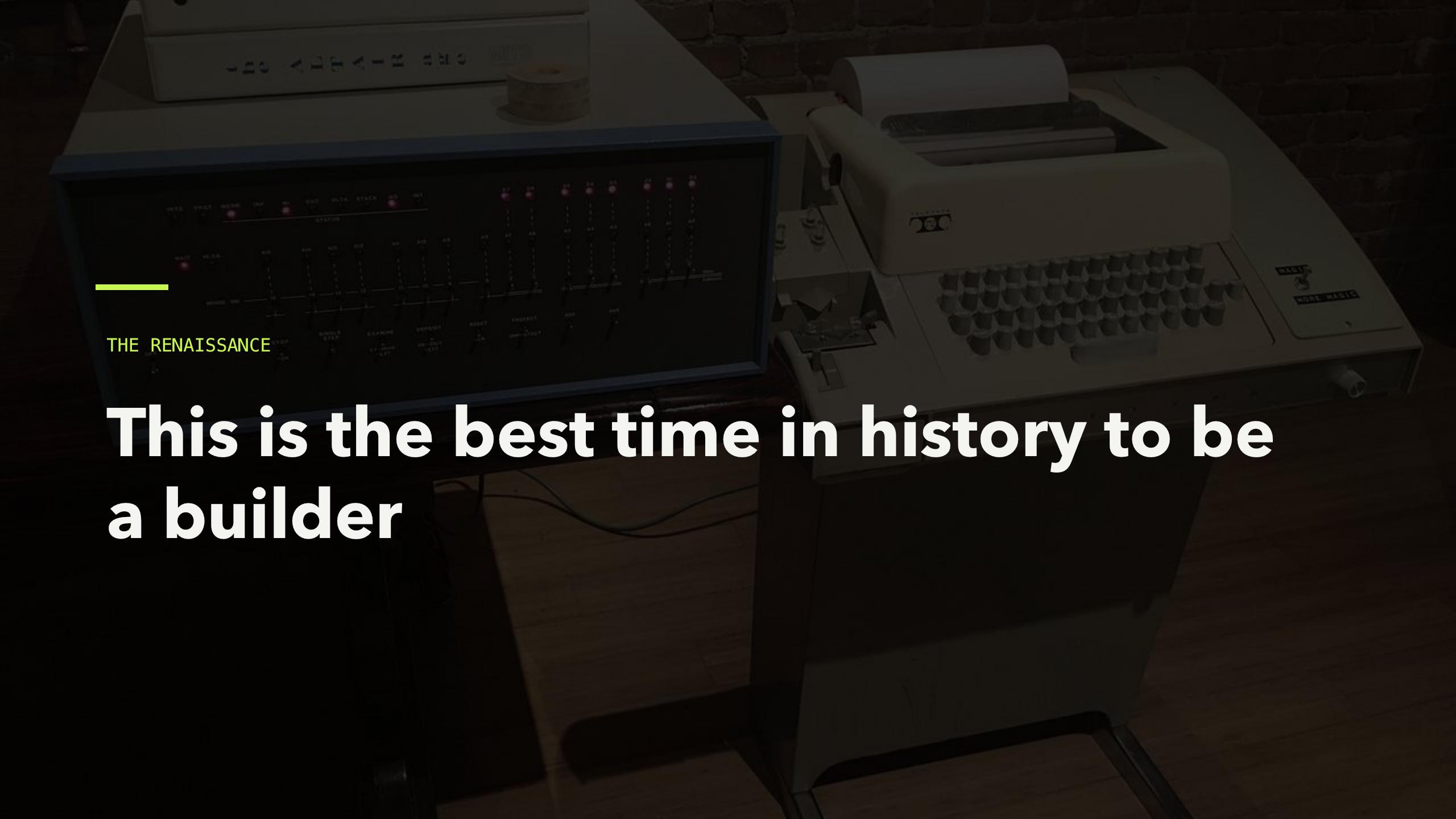
The ladder lost its bottom rung



WHAT THAT MEANS

The ceiling did not move



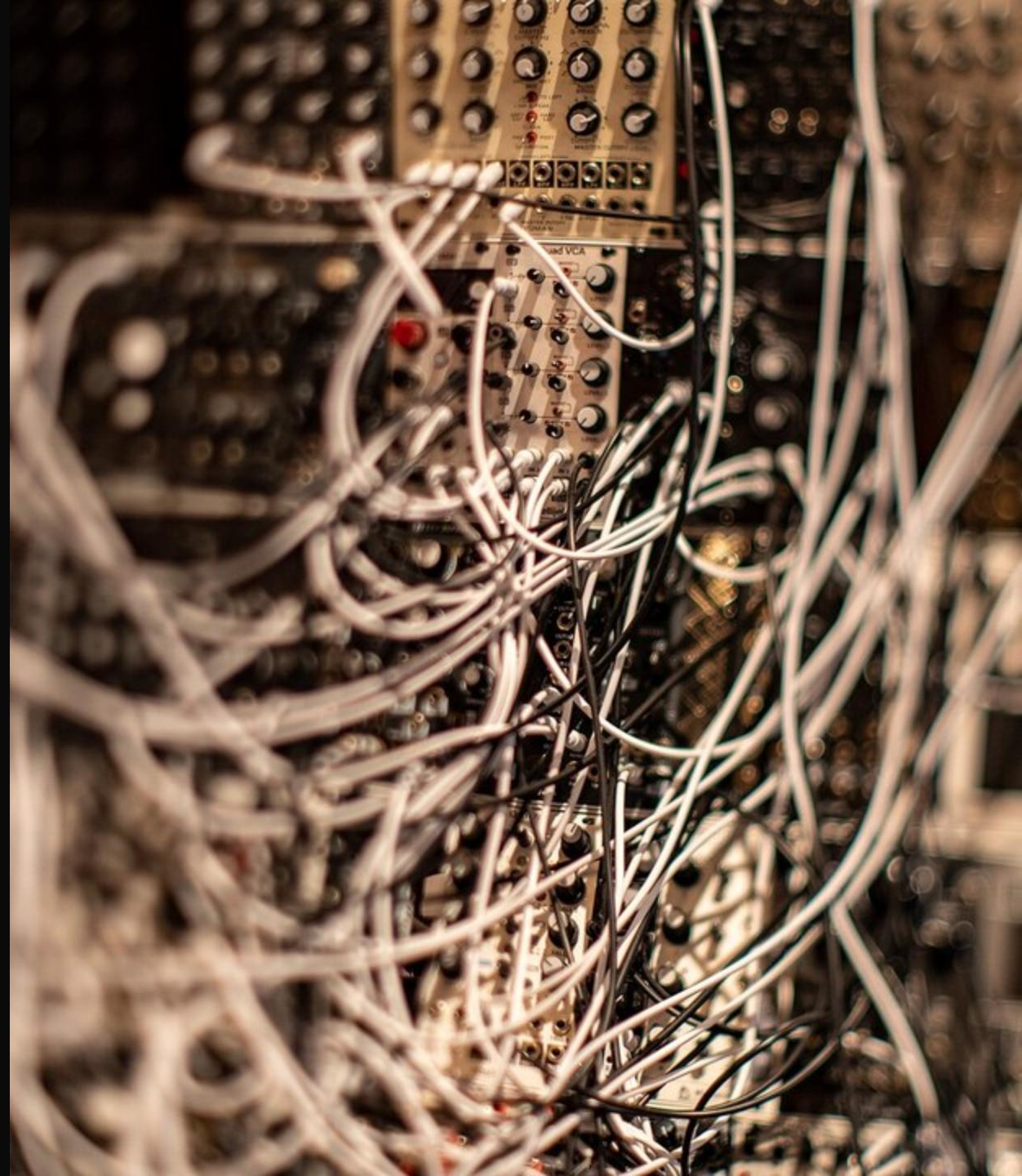
The image shows a vintage computer setup on a wooden desk. On the left is an Altair 8800 microcomputer, a dark-colored box with a control panel featuring numerous toggle switches and indicator lights. Above the computer, a white box is labeled "100 ALT AIR 8800". To the right of the computer is a teletype terminal with a roll of paper and a keyboard. The background is a brick wall.

THE RENAISSANCE

**This is the best time in history to be
a builder**

MAKERS

The pendulum swung back to people who make things



WHERE TO POINT IT

Problems worth your next ten years



Agent identity and permissions, which nobody has solved. Machine generated code arriving faster than anyone can review it. Medical devices, industrial control systems, the radio spectrum. Everything that was never connected before is being connected now, and most of it has never been looked at by anybody who knows how to break it.

Source: Check Point Research

DEFENCE

The defenders got the same upgrade



MONDAY

What to do with the next ninety days



FULL CIRCLE

The kid with a laptop in Cebu can reach the frontier



THE RECEIPTS

What I built while I was telling you this

SAGE

Governed memory for AI agents. 248 stars. The last slide is about this.

LevelUp

Agentic capture the flag, live at levelupctf.com. The next slide is about this.

mynah

Voice operated agent manager for a SAGE federation. Speak from anywhere you are.

CFP Directory

Call for papers platform connecting speakers with events. Live at cfp.directory.

QuietType

Dictation for macOS that transcribes on the machine. Nothing leaves your Mac.

Go build something

Thank you. Questions welcome.

Dhillon "@L33tdawg" Kannabhiran

@L33tdawg · github.com/l33tdawg

SCAN TO FIND ME



github.com/l33tdawg