Morning Intel — Tuesday, February 17, 2026

TL;DR

- **Security alert:** 18K OpenClaw instances exposed, 15% of community skills found malicious — audit our setup immediately
- **Chrome previews WebMCP** — AI agents get native structured web access, could replace scraping workflows
- **Voicebox drops:** local voice cloning via Qwen3-TTS — no cloud, directly relevant to our TTS stack

🔥 Top 5 Highlights

No.	Item	Rating
1	**OpenClaw Security Audit** — 18K exposed instances, ~15% of community skills contain malicious instructions (malware, exfil, cred theft). Direct concern for us.	★★★★★
2	**Chrome WebMCP Preview** — Google previewing protocol for AI agents to interact with websites natively via structured APIs. Game-changer for browser automation.	★★★★★
3	**AGENTS.md Research Paper** — arxiv paper evaluating whether AGENTS.md files improve coding agents. 102 HN points, 71 comments. Validates our approach.	★★★★★
4	**Voicebox @ hasantoxr** — Local voice cloning powered by Qwen3-TTS. No cloud, no subscriptions. 3.7K likes. Potential upgrade for our TTS pipeline.	★★★★★
5	**OpenClaw Cost Reduction Guide @ KSimback** — Full guide to cutting model costs by 90%. We run overnight swarms — savings compound fast.	★★★★

📚 New Bookmarks (2 new of 240 total)

No.	Author	Tweet	Type	Summary
1	@austin_hurwitz	"Turn Your OpenClaw Agent into a Self Improvement Machine"	Skill/Guide	Daily AI self-improvement digest — cron job scanning curated sources, setup review against existing infra, experiment tracking
2	@adriansolarzz	"how to turn nano banana pro + grok imagine + IG into a $100M machine"	Sales pitch	AI deepfake video + IG verified account network. Promotional content, ethically questionable targeting

No.	What This Means	Deep Analysis	Action Items
1	Meta-learning loop for agents — compare new findings against your own setup and improve	Self-referential improvement cycle with experiment tracking, deduplication, grounded suggestions. Adds a layer we don't have.	Adapt "Setup Review" pattern into our workflow. Adopt experiment tracking schema. Add missing sources (Lilian Weng, Geoff Huntley).
2	AI deepfake outreach is happening in the wild at scale	Sales funnel disguised as strategy. Targets older demos	Skip. Note as trend data point only.

		who “can’t detect AI.” ToS-violating account networks.	

🔥 **Highlights:** @austin_hurwitz self-improvement skill — the setup review pattern is gold

💡 **Cool Stuff:** The experiment tracking schema could level up our memory system

🤷 **Less Useful:** @adriansolarzz deepfake outreach — promotional noise

📡 Timeline Discoveries — 20 Posts Captured

Top finds from the For You feed:

No.	Author	What
1	@hasantoxr	Voicebox: local voice cloning via Qwen3-TTS. No cloud. 3.7K ❤️
2	@getdelve	AI agents closed SOC 2 audit in 19 days (was months). 8.9K ❤️
3	@chrysb	5 ways OpenClaw will shoot you in the foot — agent drift, state scatter, rule enforcement
4	@KSimback	Reduce OpenClaw costs by 90% — full optimization guide. 1.8K ❤️
5	@Legendaryy	OpenClaw v2026.2.15: Telegram streaming mode + topics no longer required
6	@supermemory	Knowledge graph + hooks for OpenClaw memory. Worth evaluating vs QMD
7	@codyschneiderxx	Claude Code + Instantly AI = speed-of-thought outbound automation
8	@patrick_oshag	Software moats in the AI era — vertical defensibility analysis
9	@Lukealexxander	YC asking people to start AI-native agencies — step-by-step guide
10	@froessell	How to build apps that don’t look vibecoded. 4.1K ❤️

Threads worth reading: @chrysb on agent drift pitfalls, @KSimback cost reduction guide, @hooeem 30 NotebookLM use cases

Timeline vibe: Heavy OpenClaw night — ecosystem maturing with memory plugins, streaming, operational wisdom. Strong “agents in production” energy.

🔧 GitHub Trending

No.	Repo	Stars	Why Interesting
1	rowboatlabs/rowboat	7,461 (+700)	Local-first AI coworker with knowledge graph + MCP. Comparable to our Claw architecture.
2	ChromeDevTools/chrome-devtools-mcp	Trending	Official Chrome DevTools MCP server. Superior to our stealth-browse stack for debugging.
3	letta-ai/letta-code	1,532	Memory-first coding agent with skill learning from trajectories. Similar to our AGENTS.md approach.

4	p-e-w/heretic	6,611 (+891)	Automatic LLM censorship removal. Fastest growing. Controversial but notable.
5	gsd-build/get-shit-done	15,019 (+436)	Meta-prompting & spec-driven dev for Claude Code. May have patterns better than our AGENTS.md.
6	hesreallyhim/awesome-claude-code	23,975	Curated Claude Code skills, hooks, plugins. Mine for additions.
7	max-sixty/worktrunk	2,149	Git worktree management for parallel AI agent workflows.

Trends: Claude ecosystem exploding (3 repos). Memory-first agents emerging. MCP becoming standard integration layer. Git worktrees for multi-agent dev.

📰 News & Trends

No.	Story	Rating
1	**Chrome WebMCP** — AI agents interact with websites via standardized protocol. 367 posts on X.	★★★★★
2	**AGENTS.md Research Paper** — Academic evaluation of agent instruction files. 102 HN pts.	★★★★★
3	**OpenClaw Security Audit** — 18K exposed instances, 15% malicious skills. Reddit r/ML.	★★★★★
4	**Bluetooth Privacy (Bluehood)** — Devices leaking identity via BLE advertising. 417 HN pts.	★★★★
5	**Kimi Claw by Moonshot AI** — Cloud-hosted OpenClaw agent. 37K posts on X.	★★★★
6	**FreeFlow STT** — Free Wispr Flow alternative by Zach Latta. 183 HN pts.	★★★★
7	**NanoClaw in Docker Sandboxes** — Official Docker blog on isolated agent execution.	★★★★
8	**Claude Code DevTools** — Local log viewer for debugging agent interactions.	★★★★

Macro trends: Agent security is THE topic (exposure + sandboxing + supply chain). MCP expanding rapidly. AGENTS.md going mainstream. Voice/STT commoditizing.

⚡ Action Items

Pri	Action	Source
🔴	Audit our OpenClaw security posture — check exposure, review installed skills for malicious content	News #3
🔴	Evaluate OpenClaw v2026.2.15 upgrade — Telegram streaming mode is a direct improvement	Timeline #5
🟡	Add Chrome DevTools MCP to our config — official Google MCP for browser control	GitHub #2
🟡	Read the AGENTS.md research paper — validate/improve our approach	News #2
🟡	Evaluate Voicebox for local voice cloning — potential TTS pipeline upgrade	Timeline #1

🟡	Adopt “Setup Review” pattern from @austin_hurwitz skill — meta-learning for our morning pipeline	Bookmark #1
🟡	Review @KSimback cost reduction guide — optimize overnight swarm spend	Timeline #4
🟢	Explore rowboat knowledge graph architecture — compare with our memory system	GitHub #1
🟢	Check awesome-claude-code for skills/hooks we’re missing	GitHub #6
🟢	Evaluate FreeFlow STT as complement to mlx_whisper	News #6