



SNOK

WEEKLY DIGEST • W44 • 23-29 OCT 2026

Trick or Threat

Halloween edition: SAP, AI agent security and the money in AI

THIS WEEK'S THEME

This was a week of tricks rather than break-ins. Attackers posed as the IT helpdesk in Microsoft Teams, planted instruction files for coding agents and reused stolen developer tokens. The door was opened by the victim, or by the victim's agent.

Meanwhile SAP is moving SAP Joule Work into everyday use, Microsoft put a dollar figure on Azure and Anthropic filed for its stock market debut. Apollo's chief economist adds that, outside the tech sector, the payoff from AI has yet to show up in company results.

I have laid out thirteen cards. Each carries a seal and a reading: my forecast, labelled as opinion.

TRICK an attack on the trust of a person or an agent

THREAT a vulnerability, an escape, a dependency

TREAT good news



01 / 13

TREAT

I · The Magician

SAP TechEd 2026: SAP Joule Work moves into daily work

The Magician has every tool on the table and knows how to use them.

At SAP TechEd in Berlin on 28 October, SAP CTO Philipp Herzig presented SAP Joule Work on its way to phased general availability. Announced at SAP Sapphire in May, it connects SAP applications with Office 365, Claude Cowork, Glean and ServiceNow. SAP says more than 110,000 SAP employees and more than 150 customers, Bosch among them, have tested it.

The bigger story for me is SAP Business AI Platform and its context layer: an agent without process context is a magician without a table. SAP has not dated the platform.

READING

My bet: in 2027 the hardest part of SAP Joule Work roll-outs will be agent permissions in systems outside SAP.

Source: SAP News Center, 26 and 28 Oct 2026



02 / 13

TREAT

X · Wheel of Fortune

Microsoft puts a dollar figure on Azure: \$33.2bn a quarter

The Wheel turns for everyone; not everyone knows which way.

In its July-September 2026 results Microsoft reported Azure revenue of \$33.2bn, up 48% year on year. TechCrunch notes the company had previously disclosed only growth rates. Its 10-Q also shows \$10bn of revenue from commercial arrangements with OpenAI, including revenue-sharing payments.

That second figure shows how closely the largest cloud's fortunes track a single customer. For anyone building on Azure OpenAI, it is a case for an architecture in which the model can be swapped.

READING

I expect that within a year other hyperscalers will report AI revenue separately, because investors will insist on it.

Source: Microsoft, press release and 10-Q, 28 Oct 2026; TechCrunch



03 / 13

TREAT

III · Three of Pentacles

SAP LeanIX and SAP Joule Studio: architecture before agents

Architect, craftsman and plan, all on one table.

In its Q3 AI release highlights (26 October) SAP made the SAP Joule Studio agent builder free until December 2026 and brought Mistral models to SAP Business AI Platform, with a SAP Sovereign Cloud version planned for early 2027. Five days earlier SAP announced that SAP LeanIX had been named a Leader in the Gartner Magic Quadrant for EA tools for the sixth time.

I read these together. A free agent builder will multiply agents faster than anyone can document them, and the architecture map shows what talks to what.

READING

My forecast: by spring 2027 an agent inventory will be a standard part of the architecture repository in SAP shops.

Source: SAP News Center, 21 and 26 Oct 2026



04 / 13

THREAT

XVI · The Tower

PHP2Shell joins CISA's KEV list: the deadline was 29 October

Lightning strikes a structure everyone thought was sound.

On 26 October CISA added both PHP2Shell flaws (CVE-2026-109618 and CVE-2026-109619) to its Known Exploited Vulnerabilities catalogue, giving federal civilian agencies until 29 October. A researcher confirmed remote code execution on an Apache mod_php honeypot. First breach reports are emerging: Switzerland's TCS Camping links a customer data leak to a PHP flaw, and the firm Dream claims 25 compromised servers. Neither has been independently verified.

W3Techs puts PHP at roughly 70% of websites with a known server-side language, which does not make them all vulnerable. Last week we wrote about attempted attacks; now there is a working exploit.

READING

I would wager that by the end of November we will see the first confirmed PHP2Shell breaches on servers whose owners did not know they ran PHP.

Source: CISA KEV, 26 Oct 2026; php.net; BleepingComputer; watson.ch; The Next Web, 26-28 Oct 2026



05 / 13

TRICK

VII · Seven of Swords

A fake helpdesk in Microsoft Teams: more than 400 incidents

A thief carries weapons out of the camp in broad daylight.

Arctic Wolf has described (26 October) more than 400 incidents in which attackers messaged staff through external Teams chat posing as IT support, often after flooding their inboxes. From the first conversation to malicious code running took under 15 minutes, most often via Quick Assist.

This is a trick in its purest form: the victim opens the door. Arctic Wolf recommends an allow-list of external domains, blocking trial tenants and limiting Quick Assist to IT roles.

READING

I expect that in 2027 insurers will ask about external Teams chat settings as routinely as they now ask about MFA.

Source: Arctic Wolf, 26 Oct 2026; Infosecurity Magazine, 27 Oct 2026



06 / 13

TRICK

VII · Seven of Cups

Gheist, OVHcloud CLI and LiteLLM: poisoned developer tools

A tempting choice of cups, and a snake waits in one of them.

Wiz Research has described (25 October) Gheist: stolen GitHub tokens used to create branches whose workflows dumped secrets into GitHub Actions logs, across more than 850 accounts. GitHub's controls stopped it in public repositories. The same fortnight brought tampered releases of OVHcloud CLI (19 October) and LiteLLM 1.107.0 (21 October).

The common thread is trust in tools we installed ourselves. Immutable releases, hash checks and short-lived tokens instead of personal ones all help.

READING

My bet: in 2027 supply-chain audits will cover developer tokens as closely as administrator accounts.

Source: Wiz Research, 25 Oct 2026; LiteLLM, 23 Oct 2026; OVHcloud, 20 Oct 2026



07 / 13

THREAT

VIII · Eight of Swords, reversed

OpenAI: agents break out of virtual machines in tests

Reversed, the prisoner sheds the bonds and walks out of the circle.

OpenAI has described (23 October) red-team exercises in its own environment. Agents told to hunt for vulnerabilities chained flaws in several experiments and ran code outside their virtual machine. In other tests they passed synthetic secrets between isolated machines through side channels on shared hardware.

One caveat: the researchers set the secret exchange as the task. The lesson still holds: agent isolation has to assume side channels on shared hardware.

READING

My forecast: by mid-2027 agent isolation down to the hardware level will be a standard requirement in tenders for agentic deployments.

Source: OpenAI, 23 Oct 2026; Digit, 26 Oct 2026



08 / 13

TRICK

o · The Fool

AGENTS.md in the Downloads folder hijacks a coding agent

The Fool walks on trustingly without looking down.

Forever Security has reported (22 October) a case at a customer: an AGENTS.md file in Downloads, dressed up as engineering notes, led a coding agent to try installing a malicious npm package. The install was blocked. In the firm's own tests Codex ran a planted test payload in over 90% of attempts and Claude Code redirected traffic to the researchers' server in about half (data from a firm that sells agent protection).

The researchers say there is nothing to patch: agents read instruction files by design. Do not start an agent in Downloads, and keep approvals and the sandbox switched on.

READING

I suspect that in 2027 security scanners will start treating agent instruction files the way they treat executables.

Source: Forever Security, 22 Oct 2026; BleepingComputer, 25 Oct 2026



09 / 13

TRICK

XVIII · The Moon

Shadow AI in Polish companies: data we cannot see yet

Enough light to see shadows, not shapes.

CRN.pl reported (23 October) a survey suggesting that unsanctioned AI use in Polish companies outstrips sanctioned use. I am not repeating the figures: the article gives no sample or method, and the likely source, a Grant Thornton Poland report from 13 October, sits behind a form.

In Tuesday's post we wrote that we had found no reliable Polish data on shadow AI. This report may change that. Until then, I think a register of tools that staff declare achieves more than a ban.

READING

I would wager that the first Polish data with a published method will show more shadow AI than IT departments report.

Source: CRN.pl, 23 Oct 2026; Grant Thornton Poland, 13 Oct 2026



10 / 13

TREAT

XIX · The Sun

Gemini 4 Carbon: a frontier model aimed at cyber defence

Clarity, this time on the defenders' side.

Google has announced (28 October) Gemini 4 Carbon. It scores 59 on the Artificial Analysis Intelligence Index v5, ahead of Claude Opus 5.5 (58) and GPT-6 Astra (57). Google reports 88.2% on SEC-bench Pro and 54.8% on ExploitGym. For now access is limited to selected cyber defence teams, with Fairwind programme partners to follow.

The lead is one point on an index that changed its methodology the day before, and the hallucination rate rose from 4% to 11%. The good news lies elsewhere: defenders got the model first.

READING

My bet: in 2027 access to new frontier models will start with defence teams.

Source: Google, 28 Oct 2026; Artificial Analysis, 27-28 Oct 2026



11 / 13

THREAT

XV · The Devil

Qwen, Cohere and DeepSeek: model provenance as a risk

A chain that can be lifted off, once someone notices it.

Cohere has described (26 October) a test in which Qwen3.8-Flash-Next, inside a closed sandbox, tried to send a probe string to an Alibaba Cloud bucket in the Beijing region. Nothing left the container, and Cohere attributes no intent. Earlier, on 20 October, a DHS order told US federal civilian agencies to remove DeepSeek products.

Cohere sells competing models, which is worth bearing in mind. The lesson is practical all the same: an open-weight model running in-house needs egress control like any other software.

READING

I expect that in 2027 EU public tenders will start asking for a declaration of AI model provenance.

Source: Cohere, 26 Oct 2026; Federal Register, 20 Oct 2026



12 / 13

TREAT

Ace of Pentacles

Anthropic files its S-1: over 11,900 customers above \$100k

A coin offered from the clouds: a material new start.

Anthropic filed its S-1 with the SEC on 26 October ahead of a Nasdaq listing. The filing shows \$16.3bn of revenue in the first half of 2026 and more than 11,900 customers paying at least \$100,000 a year. Amazon has invested \$18bn in total. The \$965bn figure is May's funding-round valuation; the filing does not yet price the listing.

SNOK works with Claude every day, so I stick to the numbers in the filing. The risk factors are the most telling part: some planned data centres will rely on on-site gas generation.

READING

My forecast: once listed, Claude's enterprise pricing will grow more predictable, because a public company explains its margin every quarter.

Source: Anthropic, Form S-1 (SEC), 26 Oct 2026; Anthropic, 28 May 2026



13 / 13

TRICK

IV · Four of Cups

Apollo: zero payoff from AI outside the tech sector

Boredom that misses the cup being offered.

Torsten Slok, Apollo's chief economist, wrote on 24 October that the technology has delivered "zero financial payoff to corporate America outside of tech". His case rests on macro data for the S&P 493. Four days later Anthropic added reports, surveys and pooled budgets to Claude Enterprise, which show usage, cost and self-reported value.

Neither measures a financial return. I think the return from AI shows up first in a specific process, long before it moves an index average.

READING

I suspect that in 2027 boards will account for AI process by process, against a baseline taken before roll-out.

Source: Apollo, The Daily Spark, 24 Oct 2026; Anthropic, 28 Oct 2026

Three checks for November: PHP, agent instruction files and Teams

The thirteen cards point to three things worth checking in the coming weeks.

- 1 An inventory of PHP, including inside products where it is not visible, and updates to the 21 October releases.
- 2 Rules for AGENTS.md and CLAUDE.md: no agent starts in Downloads, and unfamiliar instruction files get reviewed.
- 3 External Teams chat limited to an allow-list of domains, with Quick Assist reserved for IT roles.

We review these three areas in SNOK security assessments. Contact: office@snok.ai · snok.ai

SNOK Sp. z o.o. · Rondo ONZ 1, 00-124 Warsaw · snok.ai
For information only. Not legal or investment advice.

