



SNOK

WEEKLY DIGEST • W38 • 11-17 SEP 2026

Not the tool, the route

Ten items from the week, with a note on what each one changes in your systems

THEME OF THIS ISSUE

The SAP Security Patch Day of 8 September carried a note rated 9.8. Four days later a public description of the mechanism existed, and that same evening there was a working proof in a lab. This is not a story about one vulnerability - it is the first of ten items in which the decision was never which tool to buy.

Every time it was a different question: which route to take. Patch the kernel or tighten an internal communication parameter. Monitor one route to bank details or all eight. Give the agent a document in an index or a live record. These decisions are made once, usually early, and usually alongside something else.

96 hours from note to proof

8 routes to the same field

24 contract clauses for AI

Ninety-six hours from the note to working code

The SAP Security Patch Day of 8 September carried note 3759472. The flaw sits in the SAP Message Server: nothing verifies authenticity when a gateway entry is written, so an unauthenticated client supplies its own host and port and the kernel broadcasts that identity to every application server.

Four days later a public kernel diff analysis appeared, and the same evening the research team had a working proof. An AI coding assistant helped reconstruct the data format, which the researchers state openly. Rated 9.8, HotNews, no workaround.

TAKEAWAY

**The quarterly patch window no longer matches reality
- the distance to public code is counted in days.**

Kernel line 9.x is mainstream S/4HANA; the 7.x and 8.x kernels lack this command family.

Source: SecurityBridge Research Lab and Onapsis, SAP Security Note 3759472, September 2026

Eight routes to the same field

In a vendor demonstration, bank details were changed by eight different routes - alternative transactions, transport mechanisms, custom development, interfaces and background processes. None raised an alert, because monitoring covered the intended route, the standard transaction.

The second argument adds time. SAP security sits where network security sat twenty years ago: able to detect and report, unable to stop. What an attacker needs is the gap between the alert and a human response.

TAKEAWAY

A role list tells you who may come through the door. It does not tell you who came through the window.

The figure of eight describes one demonstration environment, not a property of the system.

Source: SecurityBridge, Breaking the Rules and the bank details webinar, 2026

Seventy-eight instruction files and six thousand stars

A public GitHub package turns a coding assistant into an offensive working tool. We counted the repository ourselves: 78 instruction files across 23 categories, loaded on demand. The repository was created in March and already carries 6,011 stars.

The mechanism matters more than the package. This is not an exploit to compile, it is a set of text files someone drops into an assistant's directory. The attack surface grows by a ready-made methodology, not by a new tool.

TAKEAWAY

Someone else's agent instruction file is untrusted code, not documentation. Procurement policy does not cover this case.

Gate before installation: agent skill scanning for prompt injection and data exfiltration.

Source: Repository SnailSploit/Claude-Red, metadata retrieved 17 September 2026

Almost three thousand commands in a distribution package

A classic launcher for penetration testing commands has been rewritten in Go and packaged into the official Kali Linux repositories. The project description lists 247 tools, 2,926 commands and more than two hundred cheat sheets.

This is not a new attack engine, it is a productivity layer over tools that have existed for years. Set beside the previous item, it shows the barrier to entry dropping through two independent channels at once.

TAKEAWAY

Defence is planning against an opponent who no longer has to remember syntax or the order of steps.

We measured the project metadata; the tool and command counts come from its description.

Source: Repository [halilkirazkaya/arsenal-ng](https://github.com/halilkirazkaya/arsenal-ng), metadata retrieved 17 September 2026

Grounding on documents answers a different question

UiPath has described a layer through which an agent reaches live records in the customer's systems instead of working on vectors built from documents. Four requirements: current state, structure that allows filtering and joining, entity models built once, and permissions and lineage by default.

Similarity search will answer what the returns policy says. It will not answer which tickets in a region are overdue, because that is a query with a filter and a join, and the answer is a number computed from rows.

TAKEAWAY

A project that starts with document vectorisation ends with an agent that is eloquent and inoperative.

Vendor material - the range of supported systems is not listed in it.

Source: UiPath, material on the Data Fabric layer, September 2026

Three orchestration patterns on one engine

Orchestrator manages the workers; Maestro runs the process those workers are part of. Underneath sits a durable execution engine, so a process paused on an approval resumes exactly where it stopped and survives the failure of the system it depends on.

Three patterns sit on that engine. Structural, in process modelling notation, when the path is known in advance. Code-first, when the logic reads better in a repository. Adaptive, when the next step cannot be predicted at design time.

TAKEAWAY

The pattern follows from the process, not from the consultant's preference. Getting it wrong costs a rewrite.

The developer canvas is in public preview; the source gives no general availability date.

Source: UiPath, product material on Maestro and Maestro Flow, September 2026



07 • UIPATH • BUILDING AGENTS

Three routes and the cost of picking the wrong one

The three routes to building an agent are equals: the Python software development kit, agents coded through the command line, and the browser canvas. The vendor material describes all three as first-class and does not say which to open first.

This is not a matter of taste. It decides how much control the team takes. The development kit gives the most freedom and the most labour. The canvas gives the fastest start and the least say over detail. The command line keeps the code under version control.

TAKEAWAY

**Discussing the route at the start costs an hour.
Skipping it costs a rebuild.**

A project does not move between routes without being rewritten.

Source: UiPath, material on routes to building an agent, September 2026

Quadrant leader and a deployment with numbers

A second consecutive year as a leader in the analyst quadrant for document processing; the report is dated 8 September. Alongside it, a case study from a telecommunications operator: three agents in production, robots acting as the agents' tools.

The knowledge assistant answers in seconds instead of days and removes 25,000 to 30,000 manual hours a year. The hardest objection is a different one: are we buying technology on its way out. Producing an answer is not the same as closing a process.

TAKEAWAY

Validation, approval thresholds and audit trails are execution problems, not intelligence problems.

The analyst firm does not endorse vendors, and its publications are opinions, not statements of fact.

Source: UiPath investor announcement and the PLDT case study, September 2026

Twenty-four clauses and the question of who carries risk

A practising lawyer has assembled a catalogue of contract provisions for two roles: eighteen protecting the party deploying the system and six protecting the provider. On the deploying side the same points recur - no training on user data, notification of changes, and genuine human oversight.

Three remarks from the discussion weigh more than parts of the list. Training is not retention. Change notification must cover a swap of the underlying model. Contractual liability does not replace confirmation that the system may be used today.

TAKEAWAY

Compliance moves from the slide deck to the contract annex, where the parties' interests diverge.

This is not legal advice - the interpretations require review by a lawyer before use.

Source: A practitioner's series of posts and the AI Act, article 113 as amended, 2026

A hundred and eighty billion parameters at a desk

A dense model of 27 billion parameters fits in roughly 17 gigabytes after four-bit quantisation and carries a native context of 262,000 tokens. A community recipe serves a sparse variant of 180 billion parameters on a single desk-class device.

The second point is less striking and more important. Three variants of the same family carry three different licensing regimes, including one with a revenue threshold and one that excludes serving the model as a service.

TAKEAWAY

The sovereignty conversation stops being a choice and becomes arithmetic. The licence is checked before the quote.

The speeds come from one author's recipe description - this is not our own measurement.

Source: The Qwen3.8-27B model card on Hugging Face and a community recipe, 14 September 2026



One sentence for this week

In ten items the decision was never about which tool to buy. It was about the route: a kernel patch or an internal communication parameter, one monitored route or all eight, a document in an index or a live record. Each of those decisions is made once, and it decides who answers for it later, what it costs and how fast you can react.

snok.ai

Full write-ups at snok.ai • Questions: office@snok.ai

Informational material. Not legal or investment advice.