THE CYBER TOOLCHAIN

NO. 025

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED JULY 25, 2026 · EVERY DAY

The daily firehose — everything the toolchain shipped today, already filtered.

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 17 tools

APPLICATION SECURITY

vim ? help

◆ SAST / SCA / Code Security

Cloudsmith ⓘ changelog · Jul 25, 2026 CHANGELOG ↗

Cloudsmith is a cloud-native, universal package management platform that enables teams to securely host, manage, and distribute software artifacts across multiple formats.

Cloudsmith CLI gains automatic OIDC auth and Docker credential discovery; cooldown policies expand to Maven packages.

- Introduces a Docker credential helper in the CLI to automatically authenticate to Cloudsmith registries.
- Extends cooldown policies to Maven packages, enabling supply-chain protection against newly published versions that haven't undergone sufficient scrutiny.

WAS THIS USEFUL? 👍 👎

◆ Secrets Detection & Management

Truffle Security trufflehog ⓘ v3.96.0 NOTES ↗ CODE ↗

trufflehog discovers, classifies, and validates leaked credentials

TruffleHog v3.96.0 adds HashiCorp Vault token, Duo API Secret Key, and SonarQube Cloud scoped token detectors plus updated Cloudflare credential format support.

└──▷ GET THIS VERSION

```
$ git clone --branch v3.96.0
https://github.com/trufflesecurity/trufflehog.git
# already have the repo? check out this version:
$ git checkout v3.96.0
```

- Adds HashiCorp Vault token detector supporting service tokens, periodic tokens, and legacy tokens with live verification against Vault's `auth/token/lookup-self` endpoint.
- Adds Duo API Secret Key detector for scanning Duo credentials.
- Adds SonarQube Cloud Scoped Organization Token detector.
- Updates Cloudflare detectors to recognize 2026+ prefixed credential formats (new `CloudflareApiTokenV2` and `CloudflareGlobalApiKeyV2` detectors).
- Adds `TargetNotFoundError` for targeted scans so consumers can distinguish definitively gone targets from transient or auth failures.

+1 more

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

ALEAPP ⓘ v2026.2.0 NOTES ↗ CODE ↗

Android Logs Events And Protobuf Parser

ALEAPP v2026.2.0 adds C2PA AI provenance parsing, Mister Skinnylegs browser artifact integration, and enhanced Samsung clipboard/CMH extraction.

└──▷ GET THIS VERSION

```
$ git clone --branch v2026.2.0
https://github.com/abrignoni/ALEAPP.git
# already have the repo? check out this version:
$ git checkout v2026.2.0
```

- New C2PA Content Provenance artifact parses AI-generated media provenance data including signer certificate, signing time, case-insensitive media path matching, and a Media State column grouping manifest rows per media file.
- New Mister Skinnylegs artifact plugin integrates browser artifact processing targeting every Chromium-based browser or browser-style app.
- Samsung Honeyboard clipboard artifact reworked with WAL recovery, SEFT support, and dual-schema handling (including old-schema UID resolution from ABX packages.xml on Android 12+).
- Samsung CMH now parsed directly from the `files` table, recovering records on Android 15 devices where the `images` view was dropped.

WAS THIS USEFUL? 👍 👎

◆ Reverse Engineering

Finite State Platform ⓘ

July 23, 2026 - Component Replacement, SBOM Export Validation, and Platform Reliabilit

BLOG ↗

Finite State Platform provides software supply chain security and firmware analysis tools to identify vulnerabilities and risks in IoT and embedded devices.

Finite State adds match evidence to findings CSV exports, carry-forward component exclusions, and modernized Bamboo/Jenkins CI/CD plugins.

└──▷ HOW TO FIND IT

After running a findings export, use the match evidence columns to identify exactly which files contain a vulnerable component and prioritize remediation.

> 📍 In the console, navigate to a version's Findings tab, click Export CSV, and open the downloaded file — each row now includes file path columns under match evidence alongside the existing vulnerability fields.

- Adds match evidence (file paths associated with each vulnerable component) to the findings CSV export, enabling precise remediation targeting.
- Carries component exclusions forward to newly scanned versions by default, reducing repeated manual configuration.
- Updates Bamboo and Jenkins CI/CD plugins to use the upgraded API, with the Jenkins plugin now published to the Jenkins Update Center.
- Queues binary scan uploads that exceed the concurrency limit instead of rejecting them, and automatically cleans up scans stuck in a started state.
- Recomputes policy violations and warnings automatically on very large versions when policy settings or vulnerability data change, without requiring a new scan.

+3 more

WAS THIS USEFUL? 👍 👎

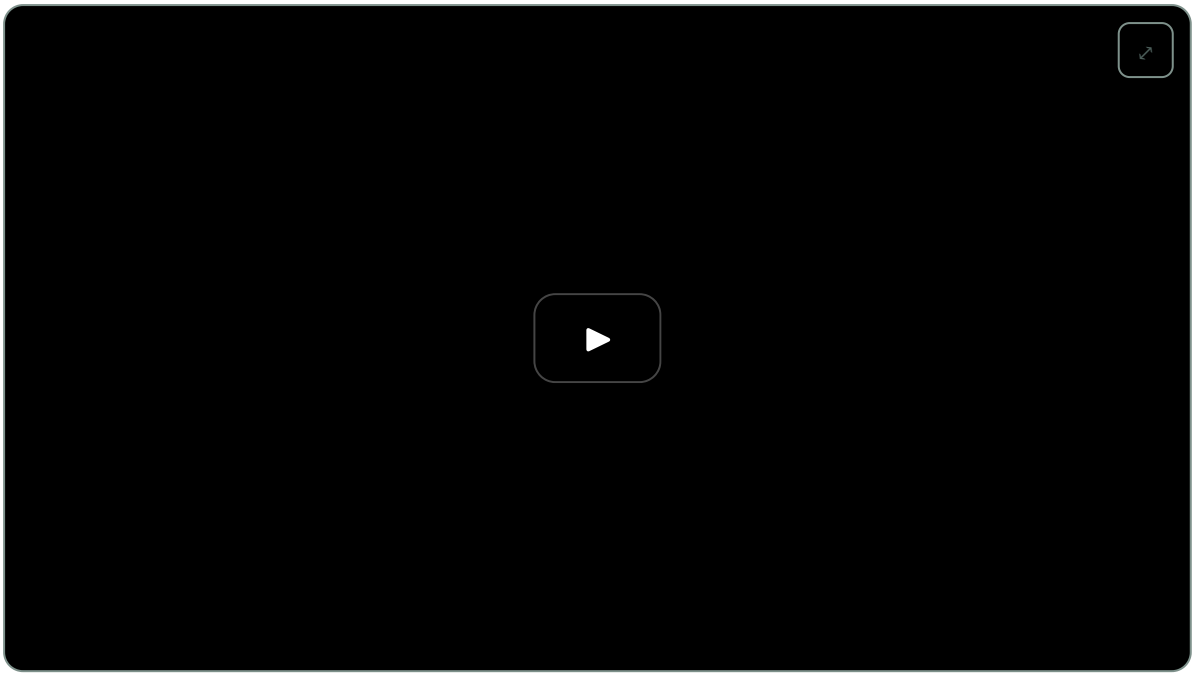
DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Iru ⓘ What's New in Iru | July 24th NOTES ↗

Manage devices and everything they touch. See how security, IT, and compliance get easier when unified around devices with Iru.

Iru adds Windows Auto App deployment for Access and token-based search on the activity page.



› New token-based search on the activity page for more precise, structured querying of activity data.

WAS THIS USEFUL? 👍 👎

◆ SOAR

Tines ⓘ

AI web search (2026-07-24) BLOG ↗

Tines is a no-code automation platform that helps security and operations teams build workflows to automate repetitive tasks and incident response processes.

Tines AI Agent actions and Workbench can now search the web, powered by Parallel.ai.

› Adds web search capability to AI Agent actions, Workbench, Workbench for Storyboard, and the App editor, powered by Parallel.ai.

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

ProjectDiscovery Cloud ⓘ

Introducing Internal Network Scanning: see your network the way an attacker inside it

BLOG ↗

ProjectDiscovery Cloud is a platform providing cloud-based security scanning and reconnaissance tools for identifying vulnerabilities and assets in applications.

ProjectDiscovery Cloud adds Internal Network Scanning to expose reachable internal assets the way an attacker inside the network would.

› New Internal Network Scanning capability scans assets from inside the network to surface reachable exposures that external scanners miss.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

ConductorOne ⓘ July 24, 2026 (2026-07-25) BLOG ↗

ConductorOne is an identity governance platform that automates access management, provisioning, and compliance across enterprise applications and infrastructure.

ConductorOne adds AI agent policy steps, access-graph search, group/role reviews, MCP per-user auth, and scoped API keys.

└──▷ HOW TO FIND IT

Set up an AI agent step in a policy to auto-evaluate low-risk access requests and reassign to super admins if it can't decide.

📍 In the console, go to Policies › [your policy] › Edit, add a new step, select Agent as the step type, set Agent mode to `Full control`, set Agent failure action to `Reassign to super admins`, and enter Agent instructions such as 'Approve if the requester is in the contractors group and the resource is tagged low-risk; otherwise deny.'

Scope a personal API key to read-only to safely hand credentials to a reporting script without granting full account access.

📍 In the console, go to your profile › API Keys › Create API Key, then open the Limit Scopes selector and choose the read-only role before saving.

Include groups and roles in a quarterly access review campaign to catch over-provisioned shared identities alongside user grants.

📍 In the console, go to Access Reviews › Campaigns › Create Campaign, open the Scope tab, and set the Grant types selector to `Users and resources` before launching.

- Adds AI Agent steps to request and review policies — configure agent mode (comment-only, full control, or policy-step changes), failure action (reassign or skip), and free-text approval instructions; evaluations appear in audit log and AI > Conversations.
- Extends request catalog search to surface entitlements that indirectly grant access to a searched resource, with a `View access graph` link showing the full grant chain.
- Access review campaigns can now scope to groups and roles (not just users) via a new Grant types selector with `Users only`, `Resources only`, or `Users and resources` options.
- Campaign templates support custom recurrence intervals (e.g. every 2 days or every 3 months) and configurable campaign run duration.
- IAM policy documents on AWS resources now render as a readable, collapsible JSON tree via a `View policy` button in resource-level access reviews and task details.

+12 more

WAS THIS USEFUL? 👍 👎

SailPoint ⓘ

Enhancement: Centered Navigation Bar for Enhanced User Experience (2026-07-24)

2 RELEASES · 2026-07-24 BLOG ↗ LATEST STABLE

SailPoint is an identity security platform that helps organizations manage and govern user access to applications, data, and systems across the enterprise.

SailPoint ISC gets a centered navigation bar for admins, end users, and Data Access Security.

- Moves the Admin tab and its megamenu to the top center of the screen for a symmetrical, at-a-glance view of all menu and submenu items.
- Relocates the + Add/Create quick-access button to the center of the main menu bar, making it reachable from anywhere on the page.
- Centers core navigation items (home icon, primary product tabs) in the header for end users to reduce eye and mouse fatigue.
- Applies the same centered navigation layout to Data Access Security, creating a consistent visual experience when switching between ISC and DAS.

▾ 1 more release in this issue · 2026-07-24

New Capability: Forms for Access Request (2026-07-24) BLOG ↗ STABLE

SailPoint ISC adds custom Forms for Access Request, collecting contextual data from requesters before submission.

- Enables admins to define custom forms and attach them to Roles, Access Profiles, or Entitlements, prompting requesters for supplementary data before submitting an access request.
- Passes submitted form data to approvers as name-value pairs, giving decision-makers full context at approval time.
- Makes form data accessible throughout the request flow, including before-provisioning rules, enabling custom provisioning logic driven by requester-supplied data.
- Automatically copies form data across multiple form instances when a requester asks for several items that each require the same form.
- Supports external access request portals (e.g., SailPoint ServiceNow Catalog Integration) by allowing supplementary form data to be passed into the request flow independent of the native UI.

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

CISO Assistant ⓘ v3.20.3 NOTES ↗

CISO Assistant is a one-stop-shop GRC platform for Risk Management, AppSec, Compliance & Audit, TPRM, BIA, Privacy, and Reporting. It supports 150+ global frameworks with automatic control mapping, including ISO 27001, NIST CSF, SOC 2, CIS, PCI DSS, NIS2, DORA, GDPR, HIPAA, CMMC, and more.

CISO Assistant v3.20.3 adds TISAX v2027, ENISA Cyber Resiliency frameworks, a Power BI native connector, Slovenian UI, and custom fields on security exceptions.

└──▷ GET THIS VERSION

```
$ git clone --branch v3.20.3 https://github.com/intuitem/ciso-assistant-community.git
# already have the repo? check out this version:
$ git checkout v3.20.3
```

- Adds TISAX v2027 framework library for automotive information security assessments.
- Adds ENISA Cyber Resiliency Maturity Assessment Framework library.
- Introduces a native Power BI connector for direct integration with CISO Assistant data.
- Enables custom fields on security exceptions, extending the existing custom-fields capability to that object type.
- Adds Slovenian (sl) language translation to the UI.

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Kiro ⓘ Claude Opus 5 Now Available NOTES ↗

Kiro is an AI-powered IDE by AWS that uses "specs" to translate requirements into structured plans, then automatically generates and implements code.

Claude Opus 5 is now available in Kiro IDE, CLI, and Web with a 1M context window and improved agentic coding performance.



└──▷ HOW TO FIND IT

Switch to Claude Opus 5 after restarting your IDE to tackle large multi-file refactors or end-to-end feature work.

📍 Restart the Kiro IDE or CLI, then open the model selector and choose Claude Opus 5.

- Adds Claude Opus 5 to the Kiro IDE, CLI, and Web model selector with a 1M token context window.
- Supports Claude Opus 5 for multi-file features, large refactors, and end-to-end feature work with self-verification and iteration.
- Enables Claude Opus 5 multi-agent coordination with fewer conflicts between parallel agents.
- Rolls out to Kiro Pro, Pro+, Pro Max, and Power customers in us-east-1 and eu-central-1 with cross-region inference at a 2.2x credit multiplier.

WAS THIS USEFUL? 👍 👎

Pi ⓘ v0.82.1 NOTES ↗

AI agent toolkit: unified LLM API, agent loop, TUI, coding agent CLI

Pi v0.82.1 adds Claude Opus 5 support, bearer auth for Anthropic-compatible gateways, and faster model catalog revalidation.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.82.1 https://github.com/earendil-works/pi.git
# already have the repo? check out this version:
$ git checkout v0.82.1
```

└──▷ TRY IT

Authenticate against an Anthropic-compatible gateway that requires bearer token auth instead of an API key.

```
$ export ANTHROPIC_AUTH_TOKEN=<your-bearer-token>
```

- Adds Claude Opus 5 model support on Anthropic and Amazon Bedrock, including adaptive thinking (with `xhigh` level), inference profiles, and prompt caching.
- Adds `ANTHROPIC_AUTH_TOKEN` bearer authentication for Anthropic-compatible gateways that require `Authorization: Bearer` headers, covering compaction and branch summaries.
- Speeds up pi.dev model catalog refreshes with `If-None-Match` conditional requests, so unchanged provider catalogs return a `304` instead of a full download.
- Exposes the `outputPad` setting to custom message renderers via the Extensions API.

WAS THIS USEFUL? 👍 👎

OpenAI Codex CLI ⓘ rust-v0.146.0-alpha.10

3 RELEASES · 2026-07-24 → 2026-07-25 NOTES ↗ CODE ↗ PRE-RELEASE

Lightweight coding agent that runs in your terminal

Adds configurable code-mode host fallback control and code-mode tool names in Responses Lite metadata.

└──▷ GET THIS VERSION

```
$ git clone --branch rust-v0.146.0-alpha.10
https://github.com/openai/codex.git
# already have the repo? check out this version:
$ git checkout rust-v0.146.0-alpha.10
```

└──▷ USE IT

Prevent silent fallback to embedded V8 so failures in the standalone code-mode host surface as tool output rather than being swallowed.

```toml
# In your Codex config file:
[features.code_mode_host]
disable_in_process_fallback = true
```

- Adds `disable_in_process_fallback` option to `features.code_mode_host` config table, letting operators prevent silent fallback to embedded V8 when the standalone code-mode host fails to start.
- Adds `code_mode_tool_names` field to Responses Lite turn metadata, exposing normalized code-mode identifier-to-ToolName mappings for each turn.
- Scopes pending network approvals to a turn and execution, coalesces duplicate requests within one execution, and assigns unique per-execution identifiers to user approval requests and permission hooks.

▾ 2 more releases in this issue · 2026-07-24 → 2026-07-25

> rust-v0.146.0-alpha.8 NOTES ↗ CODE ↗ PRE-RELEASE
>
> Codex CLI adds ent26 enterprise plan support, MCP proxy-aware auth discovery, ephemeral thread forks, and workspace plugin publish capability.
>
> └──▷ GET THIS VERSION

```
$ git clone --branch rust-v0.146.0-alpha.8
https://github.com/openai/codex.git
# already have the repo? check out this version:
$ git checkout rust-v0.146.0-alpha.8
```

- Supports the `ent26` enterprise plan tier, including authentication, rate-limit payloads, cloud-config eligibility, and usage-limit guidance.
- Routes MCP OAuth discovery and authentication status through each server's configured runtime HTTP client, enabling reliable auth for MCP servers behind proxies.
- Supports ephemeral forks of paginated threads via `thread/fork` with `excludeTurns: true`, preserving selected history and fork preview without creating a persistent rollout.
- Exposes `canPublishToWorkspace` capability metadata in plugin share contexts and `plugin/share/save` responses so clients can offer workspace-directory publishing.

`rust-v0.146.0-alpha.7` NOTES ↗ CODE ↗ PRE-RELEASE

Codex CLI adds Agent Plugins manifest support, background MCP prewarming, and paginated thread forks.

└──▷ GET THIS VERSION

```
$ git clone --branch rust-v0.146.0-alpha.7
https://github.com/openai/codex.git
# already have the repo? check out this version:
$ git checkout rust-v0.146.0-alpha.7
```

- Adds support for Agent Plugins 1.0 manifests: recognizes root `plugin.json` files and maps their metadata, `skills/`, and `mcp.json` into Codex plugin manifests.
- Applies Codex-specific apps, hooks, and interface settings from the inline `com.openai` extension in Agent Plugins manifests, with `.codex-plugin/plugin.json` as a fallback overlay.
- Adds background prewarming of MCP runtime updates so model steps are less likely to stall waiting for MCP rebuilds after config or auth changes.
- Refreshes MCP runtimes automatically when session authentication changes (auth mode, account details, or token).
- Reconnects all configured MCP servers when an explicit refresh is triggered, rather than reusing existing connections.

+4 more

WAS THIS USEFUL?

Crush

v0.87.0 NOTES ↗ CODE ↗

Glamourous agentic coding for all

Crush v0.87.0 adds MCP OAuth 2.1, Claude Channels MCP extension, and a system-wide config at `/etc` /crush/crush.json

└──▷ GET THIS VERSION

```
$ git clone --branch v0.87.0
https://github.com/charmbracelet/crush.git
# already have the repo? check out this version:
$ git checkout v0.87.0
```

- Adds OAuth 2.1 authorization support for HTTP and SSE MCP servers, unblocking MCPs that require authentication.
- Supports the Claude Channels MCP extension, allowing MCP servers to push real-time notifications into Crush.
- Supports system-wide configuration via `/etc/crush/crush.json`, improving NixOS and multi-user deployments.
- Significant LSP performance improvement: filters servers before searching `$PATH`, reducing CPU and memory usage in large repositories.
- Improves bang-mode output streaming performance by avoiding quadratic shell output rendering.

WAS THIS USEFUL?

Cline ⓘ v4.0.11 NOTES ↗ CODE ↗

Autonomous coding agent as an SDK, IDE extension, or CLI assistant.

Cline v4.0.11 adds Claude Opus 5 across six providers and Moonshot Kimi K3 support.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v4.0.11 https://github.com/cline/cline.git
# already have the repo? check out this version:
$ git checkout v4.0.11
```

- Adds Claude Opus 5 support across Anthropic, Claude Code, Bedrock, Vertex, Cline, and OpenRouter providers, including 1M context window variants.
- Adds Moonshot Kimi K3 model support.
- Includes host plugin version in all telemetry events.

WAS THIS USEFUL? 👍 👎

Claude Code ⓘ v2.1.219 NOTES ↗ CODE ↗

Claude Code is an agentic coding tool that lives in your terminal, understands your codebase, and helps you code faster by executing routine tasks, explaining complex code, and handling git workflows - all through natural language commands.

Claude Opus 5 lands as the new default Opus model, with 1M context, strict sandbox networking, and depth-3 nested subagents.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.1.219 https://github.com/anthropics/claude-code.git
# already have the repo? check out this version:
$ git checkout v2.1.219
```

└──▷ USE IT

Lock sandbox network access to only approved hosts so any unexpected outbound call is silently denied without an interactive prompt.

```json
# In your Claude Code settings file (e.g. ~/.claude/settings.json)
{
  "sandbox": {
    "network": {
      "strictAllowlist": true
    }
  }
}
```

Cap the depth of nested subagent spawning at 1 (flat) to reproduce pre-v2.1.219 behaviour in automation pipelines that shouldn't recurse.

```
$ CLAUDE_CODE_MAX_SUBAGENT_SPAWN_DEPTH=1 claude -p "refactor the auth module"
```

Pin the Dynamic workflow size guideline org-wide via settings so all users get it without having to touch `/config`.

```json
# In a shared settings file
{
  "workflowSizeGuideline": "medium"
}
```

- Adds Claude Opus 5 (`claude-opus-5`) as the default Opus model — 1M context window, fast mode at $10/$50 per Mtok.
- Adds `sandbox.network.strictAllowlist` setting to silently deny any sandboxed-command network request to a non-allowlisted host (no prompt).
- Adds `DirectoryAdded` hook that fires whenever `/add-dir` or the SDK `register_repo_root` control request registers a new working directory mid-session.
- Adds `mcp_server_errors` field to the headless stream-json init event, listing `--mcp-config` entries skipped by config validation; terminal runs surface a startup warning.
- Adds `workflowSizeGuideline` settings key so the Dynamic workflow size advisory can be set from any settings file (hides the `/config` row while active).

+4 more

BREAKING ON UPGRADE

- Opus 4.7 is removed from fast mode; `/fast` now applies only to Opus 5 and Opus 4.8.
- Dynamic workflows now default to a medium size guideline (fewer than 15 agents); workflows relying on the previous unrestricted default will be subject to this new cap unless overridden in `/config`.
- Managed MCP allowlist/denylist `${VAR}` entries now resolve from the startup environment and managed-settings env instead of the settings-file env, which may change which values are substituted.

WAS THIS USEFUL?

GOVERN

◆ AI/LLM Security

Daytona ⓘ Sandbox metrics and auto-pause interval support

2 RELEASES · SEEN 2026-07-25 NOTES ↗ LATEST STABLE

Daytona is a self-hosted development environment manager that automates provisioning, configuration, and management of standardized, secure dev environments across any infrastructure.

Daytona adds sandbox metrics visibility and configurable auto-pause intervals for sandboxes.

- Adds sandbox metrics to surface resource and usage data for running sandboxes.
- Supports configurable auto-pause intervals, letting users control how long a sandbox idles before pausing.

▾ 1 more release in this issue · seen 2026-07-25

> Websocket sandbox event subscriptions in SDKs NOTES ↗ STABLE
>
> Daytona SDKs gain WebSocket-based sandbox event subscriptions for real-time sandbox lifecycle updates.
>
> - Adds WebSocket sandbox event subscription support to the Daytona SDKs, enabling real-time event-driven monitoring of sandbox state changes.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · July 25, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe