THE CYBER TOOLCHAIN

NO. 033

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED AUGUST 2, 2026 · EVERY WEEKDAY

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 7 tools

OFFENSIVE SECURITY

◆ Exploitation & C2

BC Security Starkiller ⓘ 1 RELEASE · 2026-08-01 NOTES ↗

Starkiller is a Frontend for PowerShell Empire.

> Starkiller published a formal API surface and added CI-backed end-to-end testing in this window.

└──▷ **WHAT SHIPPED · 2 FEATURES** most completely described first ? what's the number?

01 **Public API documentation** NEW 35

Starkiller now publishes an API with 135 documented endpoints.

— Names endpoint count but no usage detail `0.1.0`

02 **Playwright E2E test suite in CI** NEW 35

Introduces a Playwright end-to-end test suite that runs as a CI job on every pull request. The release also adds server-side validation feedback to dynamic forms.

— Names tooling and trigger but no config detail `v3.6.0`

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

runZero

1 RELEASE · 2026-08-02 | CHANGELOG ↗

runZero is a continuous asset intelligence platform that discovers, inventories, and monitors all connected devices and software across networks in real-time.

> runZero 5.1 introduces autonomous discovery for attack surface intelligence, adds Purdue-level search across software and vulnerability inventory, and expands integrations with Git Smart Protocol scanning, Jira owner sync, and multi-sensor Tanium support.

└──▷ WHAT SHIPPED · 10 FEATURES most completely described first ? what's the number?

01 Purdue-level search in software and vulnerability inventory NEW

70

Software and vulnerability inventory now support purdue_level and lowest_purdue_level search terms, letting users filter assets by network zone level (e.g., for OT remediation prioritization).

Filter vulnerability inventory to assets at a specific Purdue level to prioritize OT remediation by network zone.

> 📍 In the vulnerability inventory search, enter: purdue_level:2

— Names exact search fields and gives a runnable query. changelog-20260802-08b87a10

THINNER COVERAGE BELOW

02 Site details page with subnet definitions NEW

55

A new site details page lets users with organization access view site details and subnet definitions without requiring admin access.

View site subnet definitions for an organization without needing admin access.

> 📍 In the runZero console, navigate to Sites, then select a site to open the new site details page showing subnets and site configuration.

— Includes exact navigation path to the new page. changelog-20260802-08b87a10

03 Goals widget Pending metric IMPROVED

50

The Goals widget now includes a Pending metric showing baseline assets that do not match the target query, with click-through to the underlying inventory.

— Explains behavior but no navigation or config detail. changelog-20260802-08b87a10

04 **AWS disabled region task skipping** IMPROVED 40

Connected AWS accounts now skip task processing for disabled AWS regions.

— Describes specific behavior change for AWS regions. changelog-20260802-08b87a10

05 **Tanium multi-sensor support** IMPROVED 35

The Tanium integration now supports specifying multiple sensors.

— Names integration and change but no setup steps. changelog-20260802-08b87a10

06 **Git Smart Protocol scanning** NEW 35

The scanner now supports services using the Git Smart Protocol.

— Names protocol supported but no usage guidance. changelog-20260802-08b87a10

07 **Jira issue owner sync** NEW 30

Adds the ability to sync issue owners with Jira.

— Names Jira integration but no configuration details. changelog-20260802-08b87a10

08 **Streamlined remediation handoffs** IMPROVED 25

Remediation handoffs are now available directly inside runZero as well as via ITSM integrations.

— Names ITSM integration but no specifics or steps. changelog-20260802-08b87a10

09 **Enhanced custom integration framework** IMPROVED 25

An enhanced integration framework with refined merge logic accelerates the building of custom integrations.

— Mentions merge logic but no mechanism or usage details. changelog-20260802-08b87a10

10 **Autonomous discovery for attack surface intelligence** NEW 15

Adds autonomous discovery for automated attack surface intelligence.

— No mechanism or scope described beyond the name. changelog-20260802-08b87a10

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Clerk

1 RELEASE · 2026-08-02 CHANGELOG ↗

Clerk is a user authentication and identity management platform that provides developers with pre-built UI components, APIs, and SDKs for sign-up, sign-in, and user management.

> Clerk shipped self-serve OIDC SSO delegation for org admins, a hosted-auth handoff method for mobile SDKs, and experimental composable building blocks for profile UI.

└──▷ WHAT SHIPPED · 3 FEATURES most completely described first ? what's the number?

01 **Self-serve OIDC SSO for org admins** NEW 90

Adds OpenID Connect provider support to Self-serve SSO, letting customers' IT admins configure custom OIDC connections directly inside <OrganizationProfile /> without needing Dashboard access. Domains are verified via a DNS TXT record and the connection is scoped to the Organization; admins must hold the org manage permission, and the capability must first be enabled per-org from Organization > Settings > Organization permissions in the Clerk Dashboard.

Delegate OIDC enterprise SSO setup to an org admin — enable the capability per organization so the Security tab appears in OrganizationProfile.

> 📍 In the Clerk Dashboard, select an Organization › Settings › Organization permissions, then toggle on "Allow this organization to set up enterprise SSO". The Security tab will now appear in <OrganizationProfile /> for admins with the org:sys_entconns:manage permission.

— Full mechanism, permission scope, and exact dashboard path given.

changelog-20260802-e58043d1

02 **Hosted auth handoff for mobile SDKs** NEW 80

A new startHostedAuth() method in the Expo, iOS, and Android SDKs hands the entire sign-in/sign-up flow to Account Portal in a browser session, automatically covering all enabled auth methods (email codes, passwords, social, enterprise SSO, MFA) without requiring any native auth UI.

Offload the entire auth flow to Account Portal from an Expo app — no native auth UI needed, all instance auth methods work automatically.

```javascript
import { useHostedAuth } from '@clerk/expo/hosted-auth'

const { startHostedAuth } = useHostedAuth()
await startHostedAuth()
```

— Names SDKs and method, includes runnable code, mechanism partly explained.

changelog-20260802-e58043d1

---

03 **Composable profile UI building blocks** NEW 66

Introduces experimental building blocks in @clerk/ui/experimental for assembling <UserProfile /> and <OrganizationProfile /> from individual panels and sections, such as UserProfileAccountPanel, UserProfileEmailSection, and OrganizationProfileMembersPanel.

Build a trimmed-down user profile page showing only the panels and sections your app needs, in the order you choose.

```javascript
import {
  UserProfileProvider,
  UserProfileAccountPanel,
  UserProfileProfileSection,
  UserProfileEmailSection,
  UserProfilePhoneSection,
} from '@clerk/ui/experimental'

export default function Page() {
  return (
    <UserProfileProvider>
      <UserProfileAccountPanel>
        <UserProfileProfileSection />
        <UserProfileEmailSection />
        <UserProfilePhoneSection />
      </UserProfileAccountPanel>
    </UserProfileProvider>
  )
}
```

— Names components and shows code, but marked experimental with little behavioural detail.

changelog-20260802-e58043d1

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Third-Party & Vendor Risk (TPRM)

Panorays ⓘ 1 RELEASE · seen 2026-08-02 NOTES ↗

Panorays is a third-party security risk management platform that helps organizations evaluate, manage, and continuously monitor the cybersecurity posture of their vendors and suppliers.

> Panorays' Q2'26 release introduces an MCP-based AI/LLM integration called Panorays Axis, upgrades Live Dashboards with new widgets and filtering, and expands the Public API for questionnaire and evidence workflows.

└──▷ **WHAT SHIPPED · 3 FEATURES** most completely described first ? what's the number?

01 **Panorays Axis MCP integration for AI/LLM tools** NEW 60

A new integration called Panorays Axis lets AI/LLM tools securely connect to a Panorays tenant via a remote MCP server, giving them access to third-party risk data through guided workflows for questionnaire analysis, assessment reports, and supplier onboarding.

— Names mechanism and use cases but no setup steps or limits Q2'26

THINNER COVERAGE BELOW

02 **Expanded Public API for questionnaire and evidence workflows** IMPROVED 57

The Public API adds new entities, endpoints, questionnaire lifecycle management, evidence validation retrieval, and additional questionnaire data fields, accompanied by updated API documentation restructured under the Panorays domain with dedicated sections for Panorays Axis (MCP) and TPCRM lifecycle use cases.

— Names concrete API surfaces but no endpoint names or examples Q2'26

03 **Live Dashboards widgets and pre-configured views** IMPROVED 38

Live Dashboards gains interactive widgets, pre-configured dashboards, and expanded filtering options for building flexible, use-case-tailored reports.

— Lists additions but no configuration detail or navigation Q2'26

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Windsurf ⓘ 1 RELEASE · seen 2026-08-02 NOTES ↗

Windsurf is an AI-powered code editor that combines an intelligent coding assistant with agentic capabilities to help developers write, edit, and debug code faster.

> Windsurf's snapshot-20260802 release centers on Plan mode with approval-gated Markdown plans, a browser preview for remote ACP agents, editable command approvals, a guided Cascade Migration Wizard, and broad multi-user Devin Cloud session upgrades, plus dozens of smaller sidebar, chat, sandbox, and hook-configuration additions.

└──▷ **WHAT SHIPPED · 27 FEATURES** most completely described first ? what's the number?

01 **Multi-user Devin Cloud session improvements** IMPROVED

85

Devin Cloud sessions now show the server-side send queue in sync with the web app (Cmd/Ctrl+Enter queues the next message server-side), display each participant's name in multi-user Slack sessions, add a 'Copy link' action to session menus, surface a 'Remote ACP is disconnected' banner with a Reconnect action when the connection drops, and allow network access requests to be granted or denied inline from chat instead of switching to the web app.

— Multiple named UI elements and shortcuts, minor gaps on triggers `snapshot-20260802`

02 **Cascade Migration Wizard for hooks/skills/memories** NEW

85

The 'Devin: Open Cascade Migration Wizard' command provides a guided wizard for chaining hooks → skills → memories migration, with per-item opt-in and dry-run previews.

Open the Cascade Migration Wizard to move existing hooks, skills, and memories to Devin Local in one guided flow with dry-run previews.

> 📍 In Devin Desktop, open the Command Palette (⌘P / Ctrl+P) and run: Devin: Open Cascade Migration Wizard

— Exact command name and dry-run behavior given `snapshot-20260802`

03 **Sandbox command exclusion config** NEW

85

A new sandbox.excluded allow/ask/deny configuration, settable at user and team level, lets specific commands run outside the Devin Local sandbox — useful for trusted build tools that break inside the proxy environment.

Configure commands that should always run outside the Devin Local sandbox — useful for trusted build tools that break inside the proxy environment.

```json
// In user or team settings (JSON)
{
  "sandbox.excluded": {
    "allow": ["make build", "docker compose up"],
    "ask": ["npm publish"],
    "deny": []
  }
}
```

— Runnable JSON config example provided `snapshot-20260802`

---

04 **Status bar hidden by default** BREAKING 80

The status bar is now hidden by default in the Agent Command Center; set "`workbench.statusBar.visible`": true in user settings to restore it.

— Exact settings key given for restoration `snapshot-20260802`

---

05 **Plan mode with approval-gated plan file** NEW 70

Plan mode in Devin Local now persists a Markdown plan file at ~/.devin/plans/plan-<session>.md and requires approval before implementation proceeds.

— Clear mechanism and file path, no toggle location given `snapshot-20260802`

---

06 **Editable command approvals with wand rewrite** NEW 70

Clicking a command in a permission approval card lets you edit it before approving, and a wand action can rewrite the command via a fast model before execution.

— Names UI path and rewrite mechanism `snapshot-20260802`

---

07 **Custom subagents as flat markdown files** NEW 70

Custom subagents can now be defined as flat agents/<name>.md files, and the per-agent directory format also accepts AGENTS.md, agent.md, and agents.md.

— Names exact file formats accepted `snapshot-20260802`

---

08 **ACU usage via /usage command** NEW 70

ACU usage is now shown via the `/usage` command in Devin Local sessions, letting users check consumption without leaving chat.

Check ACU consumption mid-session without leaving the Devin Local chat.



— Exact slash command given, minimal mechanism detail snapshot-20260802

09 **MCP server re-authentication button** NEW 65

MCP servers reporting 'Needs auth' now show an Authenticate button that clears stored OAuth credentials and reruns the browser authorization flow.

— Explains mechanism, lacks exact UI location snapshot-20260802

10 **Agent sidebar UI enhancements** IMPROVED 65

The agent sidebar gains right-click context menus, double-click rename, per-workspace filters/sort/grouping, sticky grouped spaces, and a new-session shortcut hint.

— Lists several concrete UI additions, no navigation path snapshot-20260802

11 **'Add to chat' transcript shortcut** NEW 65

An 'Add to chat' button (⌘L / Ctrl+L) lets users add selected transcript text directly to the chat input.

— Exact shortcut provided, mechanism simple snapshot-20260802

12 **Browser preview for remote ACP agents** NEW 60

Remote ACP agent sessions can now open a browser preview that proxies a local dev server, capturing selected elements and console output and sending them back to the agent as pending context.

— Explains mechanism, lacks exact activation steps snapshot-20260802

THINNER COVERAGE BELOW

13 **Devin Local Plugins section** NEW 55

A Devin Local Plugins section in customizations lists loaded plugins as well as those available from the repository, organization, or account.

— Names sources, lacks install steps snapshot-20260802

14 **Hooks tab lists configured hooks** IMPROVED 55

The Hooks tab in Devin Local Customizations now lists configured hooks along with their source and trigger events.

— Names fields shown, no navigation path snapshot-20260802

15 **ACP agents disabled in Restricted Mode** BREAKING 55

Cascade, Devin Local, and every other ACP agent are now unavailable while a workspace is open in Restricted Mode, and hooks no longer load or run there.

— Explains scope, no workaround given `snapshot-20260802`

16 **Merge button for worktree sessions** NEW 50

Worktree sessions now show a Merge button to bring changes back into the workspace, alongside existing worktree selection from the agent location selector.

— Names button, lacks deeper behavior detail `snapshot-20260802`

17 **Keyboard shortcuts for permission requests** NEW 50

New keyboard shortcuts let users always-allow or reject permission requests, with shortcut hints shown directly on the approval buttons.

— No exact key combinations listed `snapshot-20260802`

18 **Editable queued messages** IMPROVED 50

Queued messages can now be edited before they send, with @`-mentions` preserved across edits and reverts.

— Explains behavior, no UI path given `snapshot-20260802`

19 **PR tab and Devin mode visual indicators** IMPROVED 50

Pull request editor tabs now show state-specific icons (open, draft, merged, closed), and session-create cards display a Devin mode badge (Fast, Ultra, Fusion).

— Concrete states named, purely visual with no action `snapshot-20260802`

20 **Unified agent notifications setting** NEW 45

A unified notifications setting posts native OS notifications whenever any agent session finishes or needs input.

— Describes behavior, no settings path given `snapshot-20260802`

21 **Rules added to @-mention menu** NEW 45

The @`-mention` menu now includes Rules, allowing manual-trigger rules to be pulled directly into a conversation.

— Simple mechanism, minimal extra detail `snapshot-20260802`

22 **Migrate Windsurf hooks to Devin hooks** NEW 45

A new command migrates Windsurf hooks into Devin hooks across every workspace folder.

— Command exists but exact name/path not given `snapshot-20260802`

23 **Duplicate session and subagents preview toggle** NEW 40

A 'Duplicate session' action lets users branch off a conversation, and a new 'Subagents (Preview)' toggle appears in Devin settings.

— Names actions but no deeper mechanism `snapshot-20260802`

24 **Codemaps in dedicated editor tabs** IMPROVED 40

Codemaps now open in their own editor tabs in agent window mode, and codemap @`-mentions` work in Devin Local.

— States behavior, no further mechanism `snapshot-20260802`

25 **Default model for subagents** NEW 30

Subagents can now be configured with a default model.

— No config key or location specified `snapshot-20260802`

26 **Fast Context support in Devin Local** NEW 25

Fast Context support was added in Devin Local sessions.

— Name only, no behavior explained `snapshot-20260802`

27 **Timeline navigator for Devin Local sessions** NEW 20

A subtle timeline navigator was added for Devin Local sessions.

— Bare description, no mechanism given `snapshot-20260802`

╰──▷ BREAKING ON UPGRADE

! The status bar is now hidden by default in the Agent Command Center; set `"workbench.statusBar.visible": true` in user settings to restore it.

! Cascade, Devin Local, and every other ACP agent are now unavailable while a workspace is open in Restricted Mode, and hooks no longer load or run there.

WAS THIS USEFUL? 👍 👎

Cline

2 RELEASES · 2026-08-02 | NOTES ↗ | CODE ↗

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

> Cline's latest releases add conversation branching with transactional workspace rewinds, smarter Ollama cold-start handling, and model-catalog-driven reasoning controls, alongside smaller provider defaults and compatibility changes.

└──▷ **WHAT SHIPPED · 6 FEATURES** most completely described first ? what's the number?

01 **Ollama cold model load handling** IMPROVED 70

Ollama cold model loads are now supported: empty responses are retried automatically at the model boundary instead of immediately failing the task with 'Model returned empty response', and the response-start timeout is raised to 5 minutes (from 30 seconds) to allow large models to finish initializing.

— Concrete timeout numbers and retry mechanism, but no user action needed. sdk/sdk/v0.0.69 desktop-v0.0.8

02 **Edit earlier message to fork conversation** NEW 68

Users can edit any earlier message in a conversation, which forks the session at that point and rewinds the workspace to that checkpoint before re-running from the edited prompt.

— Explains mechanism (fork + workspace rewind) but no UI path given. desktop-v0.0.8

THINNER COVERAGE BELOW

03 **Reasoning controls from shared model catalog** IMPROVED 50

Reasoning controls such as effort, thinking budget, and on/off toggles are now sourced from the shared model catalog, so each model exposes only the reasoning options it actually supports.

— Describes behavior change but no config detail or example. desktop-v0.0.8

04 **Custom model info carries into seeded catalog** IMPROVED 35

Custom model info configured for OpenAI-Compatible providers now carries over into the seeded model catalog.

— Names the surface but gives no detail on how or why it matters. desktop-v0.0.8

05 **Removed R1 messages format option** BREAKING 35

The 'Enable R1 messages format' option has been removed from the OpenAI-Compatible provider.

— States the removal clearly but no migration guidance. `desktop-v0.0.8`

06 **OpenRouter default model change** IMPROVED 30

OpenRouter now defaults to Anthropic Claude Sonnet 5.

— Single fact, no further explanation of impact or override. `desktop-v0.0.8`

└──▷ **BREAKING ON UPGRADE**

! The "Enable R1 messages format" option has been removed from the OpenAI-Compatible provider.

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

goshs ⓘ 1 RELEASE · 2026-08-02 NOTES ↗

Feature-rich single-binary file server for red teamers and developers. HTTP/S · WebDAV · FTP/SFTP · SMB · LDAP/S · NTLM hash capture · DNS/SMTP callbacks · TLS · Auth · Share links.

> goshs v2.1.5 adds a password reveal popup to its TUI, letting operators retrieve basic-auth credentials mid-session without restarting the server.

└──▷ **WHAT SHIPPED · 1 FEATURE** most completely described first ? what's the number?

01 **TUI password reveal popup** NEW 88

In the `--tui` status bar, pressing `p` opens an overlay showing the basic-auth credentials; `u` toggles between masked and plaintext, `y` / `c` copies to clipboard, and `esc` / `q` closes the overlay.

When you launch goshs with a generated password and forget it mid-session, use the TUI popup to retrieve it without restarting.

```
$ goshs --tui -b "user:$(xkcdpass)"
```

— Names exact keybindings and behaviour, fully actionable. v2.1.5

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · August 2, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe