THE CYBER TOOLCHAIN

NO. 119

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED OCTOBER 24, 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

INFORMATION DENSITY

everything



BRIEFED | EVERYTHING

Every tool in the issue, in full.

all 80 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 27 tools

▾ // THE BRIEF HIDE

What stands out across today's releases, grouped by what it lets you do. Every tool named links to its entry below.

Three unrelated things stand out. Cycode gives you three canned queries to find where the compromised eMudhra intermediate CA is still ed across images, runtimes and Dockerfiles. Elastic Security Labs

vim ? help

shipped a rule for in-the-wild Zimbra Swatchdog exploitation (CVE-2026-73570). ArmorCode Zero turns grouped findings into drafted pull requests and confirms the fix by rescan.

IDENTIFY

Find every place a revoked CA is still trusted before you start pulling it

Distrusting an intermediate CA is easy; knowing which of your base images, running containers and Dockerfiles still bake it in is the part that takes a week of grep. Three prebuilt Threat Intelligence queries answer that against your own estate instead of a spreadsheet of guesses.

Cycode

DETECT

Catch Zimbra Swatchdog exploitation with a rule you did not have to write

A SIEM rule for active command injection against CVE-2026-73570, shipped while the exploitation is live. Teams that cannot patch every Zimbra host today get coverage for the attempt instead of waiting for the maintenance window.

Elastic Security Labs

PROTECT

Get a vulnerability from triaged to merged without a human in the loop

ArmorCode Zero groups findings into one fixable change, drafts the PR and re-scans to prove it closed — the dedupe-and-chase cycle that eats most AppSec time. Veracode's CLI moves static scanning and SCA dependency fixes into the developer's own workflow rather than a portal.

ArmorCode · Veracode

PROTECT

Trust your advisory feed and your crypto stack a little further

vulnerability-db adds three upstream advisory sources behind an opt-out flag and verifies database images layer-by-layer, so a truncated download fails loudly instead of silently shrinking your CVE coverage. OpenSSL 4.1.0 brings DTLS 1.3, GREASE, and post-quantum performance work to the datagram path.

vulnerability-db · OpenSSL

◆ AI-Powered Offensive Security

xalgorix

Feedback ⓘ v4.6.159 NOTES ↗ RANK

Autonomous AI pentesting agents — real-time reconnaissance, vulnerability detection, and exploitation orchestration. Go + TypeScript.

> Xalgorix v4.6.159 adds a configurable cap on idle scan iterations and improves recovery of malformed LLM tool calls to reduce wasted token usage.

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

01 Idle iteration cap for completed scan plans NEW 90

New `XALGORIX_PLAN_COMPLETE_IDLE` environment variable (default 600) bounds the no-new-findings tail after a structured plan is exhausted, finalizing scans instead of re-testing already-covered surface indefinitely; any new finding resets the counter. Can be set via shell (`XALGORIX_PLAN_COMPLETE_IDLE=100 xalgorix --web`) or persisted in `~/.xalgorix.env` .

Lower the idle-iteration cap for fast CI scans where you want earlier finalization once the plan is done and no new findings appear.

```
$ XALGORIX_PLAN_COMPLETE_IDLE=100 xalgorix --web
```

Persist a tighter idle cap for self-hosted installs that store config in `~/.xalgorix.env` .

```ini
XALGORIX_PLAN_COMPLETE_IDLE=200
```

— Named env var, default value, exact behavior and runnable examples. v4.6.159

02 Recovery of mis-tagged LLM tool calls IMPROVED 60

Xalgorix now recovers LLM tool calls where the model emits `<parameter=NAME>` instead of `<function=NAME>` , avoiding the wasted turn and full-context retry that previously occurred when such calls were discarded as malformed.

— Explains before/after mechanism but no user-facing action. v4.6.159

WAS THIS USEFUL? 👍 👎

◆ Reconnaissance & OSINT

nerva

Feedback ⓘ v1.83.0 NOTES ↗ LATEST STABLE

Fast service fingerprinting CLI for 170+ protocols (TCP/UDP/SCTP) - built by Praetorian

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v1.83.0 https://github.com/praetorian-inc/nerva.git
# already have the repo? check out this version:
$ git checkout v1.83.0
```

NEW DETECTION Citrix ADC management plane fingerprinting

NEW DETECTION elasticsearch-no-auth

NEW DETECTION Verifone VHQ and Ingenico Estate/TMS UI fingerprinting

NEW INTEGRATION pcAnywhere plugin

▾ 3 more releases in this issue · 2026-10-23

v1.82.0 NOTES ↗ STABLE

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v1.82.0 https://github.com/praetorian-inc/nerva.git
# already have the repo? check out this version:
$ git checkout v1.82.0
```

v1.79.0 NOTES ↗ STABLE

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v1.79.0 https://github.com/praetorian-inc/nerva.git
# already have the repo? check out this version:
$ git checkout v1.79.0
```

v1.78.0 NOTES ↗ STABLE

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v1.78.0 https://github.com/praetorian-inc/nerva.git
# already have the repo? check out this version:
$ git checkout v1.78.0
```

WAS THIS USEFUL? 👍 👎

myip

Feedback ⓘ v8.0.0 NOTES ↗

The best IP Toolbox. Check your IP address & geolocation, test IP for WebRTC and DNS IP leaks, run an IP quality check, browser fingerprint check, website availability check, network speed test, global latency test, MTR test, Whois search, and more.

Advanced Tools open as full pages with state preserved; reorganized into Network Diagnostics, Lookup & Calculation, and In-depth Checks; nav bar on every page.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v8.0.0 https://github.com/jason5ng32/MyIP.git
# already have the repo? check out this version:
$ git checkout v8.0.0
```

Advanced Tools now open as full pages (sliding app-style), preserving data when switching between tools.

Advanced Tools reorganized into three groups: Network Diagnostics, Lookup & Calculation, and In-depth Checks.

Navigation bar is now present on every page, making every tool one click away from anywhere in the app.

NEW DETECTION IP Blocklist Check — DNSBL and threat intelligence list coverage

NEW DETECTION Ad & Tracker Blocking Test — ad, analytics, social, and device-maker endpoint coverage

UPDATED INTEGRATION Service Status expanded to more well-known internet products

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ Secrets Detection & Management

Truffle Security trufflehog

Feedback ⓘ v3.99.7

NOTES ↗ CODE ↗

TruffleHog finds, verifies, and analyzes leaked credentials across Git, chat, wikis, cloud storage, and more

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v3.99.7
https://github.com/trufflesecurity/trufflehog.git
# already have the repo? check out this version:
$ git checkout v3.99.7
```

NEW DETECTION Fireworks AI API key detector

NEW DETECTION Infisical service token detector

NEW INTEGRATION xAI analyzer

WAS THIS USEFUL? 👍 👎

infisical

Feedback ⓘ v0.167.2 NOTES ↗ RANK

Infisical is the open-source platform for securing secrets, certificates, access, and AI Agents.

> Infisical v0.167.2 adds audit logging for secret scanning, proxy-token-based startup and default log storage for vault agents, per-signer code signing config for PKI admins, and inline folder access grants from the permissions search UI.

└──▷ **WHAT SHIPPED · 4 FEATURES** most completely described first ? what's the number?

01 **Vault agent proxy token startup and session log storage** NEW

40

Vault agent proxies can now start using a proxy token via `agent-vault` proxy token support, and a default storage configuration is added for vault agent session logs.

— Names proxy token mechanism but no config keys or defaults given v0.167.2

02 **Folder access grants from Manage Permissions search** IMPROVED

35

Folder access can now be granted directly from the Manage Permissions search UI.

— Names a concrete UI location to act from, no further detail v0.167.2

03 **Per-signer code signing config for PKI admins** NEW

25

PKI admins can now configure signer-specific code signing settings.

— States the capability without naming config fields or UI path v0.167.2

04 **Audit events for secret scanning activity** NEW 20

Infisical now logs audit events for secret scanning operations, giving operators a trail of scanning activity.

— Names the capability but no event schema or access path v0.167.2

WAS THIS USEFUL? 👍 👎

◆ SAST / SCA / Code Security

GitHub

Feedback ⓘ

Usage metrics API adds usage from tools like OpenCode (2026-10-23) BLOG ↗

RANK

GitHub is a web-based platform for version control and collaborative software development using Git repositories.

> GitHub shipped per-tool client breakdowns in the Copilot usage metrics API, a unified Copilot-powered GitHub app for Microsoft Teams, major upgrades to Public Monitoring (triage, validity checks, API, webhooks), and general availability of enterprise-level GitHub App installations with a large new set of enterprise/organization permissions.

└──▷ WHAT SHIPPED · 4 FEATURES most completely described first ? what's the number?

01 **Per-client breakdown in Copilot usage metrics API** NEW

95

Adds a `totals_by_client` array to the Copilot usage metrics API for enterprise, organization, enterprise-user, and organization-user 1-day and 28-day reports. Each entry includes `client` (e.g. `opencode`, `claude_code`, `codex`, `zed`, `copilot_cli`, `github_app`, `cloud_agent`, `code_review`, `vscode`, `jetbrains`, or `other`), `request_count`, `session_count`, and `token_usage`, plus a `totals_by_model` breakdown with a `model_selection_mode` field (`user_selected`, `auto`, `product_selected`, `other`, `unknown`); in 28-day aggregated reports `totals_by_client` also appears inside each `day_totals` entry for day-level breakdowns.

Compare model request and token volume across all Copilot-connected tools in your org to inform tool support and governance decisions.

```
$ curl -H 'Authorization: Bearer <token>' -H 'Accept:
application/vnd.github+json'
'https://api.github.com/orgs/<org>/copilot/metrics?report=1-day'
| jq '.totals_by_client[] | {client: .client, requests:
.request_count, sessions: .session_count}'
```

Break down per-tool usage by model and selection mode across the 28-day enterprise report to see whether developers are using auto-selected or user-chosen models in each tool.

```
$ curl -H 'Authorization: Bearer <token>' -H 'Accept:
application/vnd.github+json'
'https://api.github.com/enterprises/<enterprise>/copilot/metrics?
report=28-day' | jq '.day_totals[] | {date: .date, by_client:
[.totals_by_client[] | {client: .client, models:
[.totals_by_model[] | {model: .model, mode:
.model_selection_mode, requests: .request_count}]}]}'
```

— Full field names and values with runnable curl/jq examples

Usage metrics API adds usage from tools…

02

Triage, validity checks, API, and webhooks for Public Monitoring

NEW

95

Adds the `GET /enterprises/{enterprise}/secret-scanning/public-monitoring-alerts` REST endpoint returning alert metadata, secret type, attribution, and exposed locations, and a `secret_scanning_public_monitoring_alert` enterprise webhook event for real-time leak notifications. Adds always-on validity checks marking credentials `Active`, `Inactive`, or `Unknown`; alert management to dismiss as `Dismissed` or `Fixed` with an optional comment, reopen closed alerts, and review a full activity timeline; and enterprise dashboard filtering/sorting by repository, committer, secret type, attribution method (`membership` or `verified domain`), and state (`open` or `closed`).

Pull all open public monitoring alerts attributed to your enterprise into an incident response script or SIEM.

```
$ curl -H "Authorization: Bearer <token>" -H "Accept:
application/vnd.github+json"
"https://api.github.com/enterprises/<enterprise>/secret-
scanning/public-monitoring-alerts?state=open"
```

Subscribe your enterprise to real-time leak notifications so your pipeline is triggered the moment a new secret is attributed to your org.

> 📍 In the enterprise security dashboard, go to Settings › Webhooks › Add webhook, set the payload URL to your endpoint, and select the `secret_scanning_public_monitoring_alert` event.

— Endpoint, webhook event, and states named with runnable examples

Public monitoring adds triage, validity…

03 Enterprise-level GitHub App installations and new permissions GA

NEW

95

GitHub Apps can now be installed at the enterprise level (GA, arriving in GHES 3.24), replacing classic PATs for governance and admin automation. New permissions include `Enterprise organization and repository policies` (read/write) exposing `EnterpriseOwnerInfo` policy fields and REST APIs for repository forking, default permissions, visibility changes, creation/deletion, issue deletion, collaborator invitations, deploy keys, and protected branch updates; `Enterprise bypass requests` (read); `Enterprise settings` (read/write) via `EnterpriseOwnerInfo`; `Enterprise two-factor authentication` (read/write); `Enterprise verifiable domains` and `Organization verifiable domains` (write) for `VerifiableDomain` objects; `Enterprise IP allowlist` and `Organization IP allowlist` (read/write) for `IpAllowListEntry` and allowlist enforcement; `Enterprise access restrictions` (write); and `Enterprise repository rulesets` (write) via enterprise rules REST APIs and `RepositoryRuleset` in GraphQL. Also expands `Enterprise people` (read/write) to read `EnterpriseRepositoryInfo` via `EnterpriseOwnerInfo.outsideCollaborators`, and `Enterprise billing` (write) to update the Marketplace member purchasing setting.

Grant a GitHub App the permissions needed to manage enterprise rulesets and IP allowlists, replacing classic PAT-based automation.

> 📍 Settings › Developer settings › GitHub Apps › <your app> › Permissions & events Enterprise repository rulesets: Write Enterprise IP allowlist: Read and write Enterprise organization and repository policies: Read and write

— Every new permission and GHES version named with setup steps

`Enterprise installations for GitHub App…`

04 Copilot notifications-to-code in Microsoft Teams NEW

65

A new unified GitHub app for Microsoft Teams supports `@github` mentions in channels, group chats, and private chats to trigger Copilot actions such as investigating an issue, fixing a bug, and opening a pull request directly from a notification. It consolidates the former `GitHub notifications` Teams app and Copilot into one app; the legacy app will be renamed `GitHub (deprecated)` and retired on November 16, requiring users to install the new consolidated app.

▶ Watch video

Turn a bug-report notification into a pull request without leaving a Teams channel.

> 📍 In the Teams channel where the bug notification appeared, type: @github fix the issue in <repo> and create a pull request, then follow the prompts to connect

> your GitHub account and select a repository.

— Mention syntax and retirement date given, little mechanism detail

Turn notifications into code with GitHu…

└──▷ **BREAKING ON UPGRADE**

! The legacy GitHub app in Microsoft Teams will be renamed `GitHub (deprecated)` and retired on November 16; users must install the consolidated GitHub app to retain Copilot in Teams functionality.

WAS THIS USEFUL?  

OpenQodex

Feedback ⓘ openqodex@0.14.0 NOTES ↗ RANK

Open source code review that runs in your coding agent before you push. Scanners plus a separate AI reviewer, on your own login, no key.

> OpenQodex 0.14.0 ships a staged multi-pass review pipeline, a public graph query library API for persisting and reloading indexes, and much broader language coverage for its replaced-line behavior-loss review.

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

01 **Public graph query library API** NEW 95

Exports a public library API — `query`, `querySliced`, `OPERATIONS`, `SLICE_CHECKS`, `parseTarget`, `resolveTarget`, `prepareIndexes`, `writeIndex`, `readIndex`, `readIndexFrom`, `assemble`, `INDEX_FORMAT`, `serializeModel`, `deserializeModel`, `graphOf`, `floorReasons`, `hotSymbols`, and `isTestPath` — plus their types, so external programs can build a graph, persist the index files `writeIndex` returns (now including `projects.json`), reload them with `readIndexFrom`, and run any query over the result.

— Names every exported function and the persist/reload mechanism. openqodex@0.14.0

02 **Staged multi-pass review pipeline** NEW 80

Adds a staged review pipeline: two finder sessions read each changed file with surrounding context, a fresh verifier session checks every candidate, and only confirmed candidates become findings; style, naming, docs, and test items are surfaced separately as observations. Setting `review.stages: false` falls back to the original single-pass mode.

— Explains pipeline mechanism and names the fallback config key. openqodex@0.14.0

THINNER COVERAGE BELOW

03 **Behavior-loss review language coverage expanded** IMPROVED 55

Extends replaced-line behavior-loss review from its prior scope to cover a large set of additional file extensions, including `.c`, `.cc`, `.cpp`, `.cxx`, `.C`, `.h`, `.hh`, `.hpp`, `.hxx`, `.rs`, `.cs`, `.php`, `.ts`, `.tsx`, `.js`, `.jsx`, `.mjs`, `.cjs`, `.mts`, `.cts`, `.py`, `.pyi`, `.go`, `.rb`, `.java`, `.kt`, `.kts`, `.swift`, `.m`, `.mm`, `.scala`, `.sc`, `.sh`, `.bash`, `.zsh`, `.sql`, `.lua`, `.pl`, `.pm`, `.r`, `.R`, `.dart`, `.ex`, `.exs`, `.erl`, `.hrl`, `.hs`, `.clj`, `.cljs`, `.cljc`, `.vue`, `.svelte`, `.vb`, `.fs`, `.fsx`, `.ps1`, `.psm1`, `.groovy`, `.gradle`, `.asm`, `.s`, `.S`, `.zig`, `.jl`, `.ml`, `.mli`, `.nim`, `.v`, `.vhd`, `.vhdl`, `.f`, `.f90`, `.f95`, `.for`, `.cob`, `.cbl`, `.coffee`, `.elm`, `.el`, `.lisp`, `.lsp`, `.scm`, `.ss`, `.rkt`, `.d`, `.pas`, `.p`, `.raku`, `.tcl`, and `.awk`.

— Lists every extension but gives no new mechanism beyond coverage. `openqodex@0.14.0`

WAS THIS USEFUL? 👍 👎

Veracode

Feedback ⓘ CLI updates (2026-10-23) BLOG ↗ RANK

Veracode is a cloud-based application security platform that scans code, binaries, and running applications to find and help remediate software vulnerabilities.

> Veracode's CLI gained new commands for in-workflow static scanning and SCA-based dependency fixes, plus a wave of language-specific flags and environment variables for the `veracode package` command.

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

01 Language-specific packaging flags and environment variables

NEW 90

`veracode package` gains `--csharp-source` to package C# source directly for Static Analysis without compiling to binaries, `--skip-packagers` to exclude specific artifacts (e.g. unsupported SQL) from packaging, `--java-source` plus the `VERACODE_PACKAGE_JAVA_SOURCE=true` environment variable for Java source packaging, `VERACODE_PACKAGE_GOLANG_GENERATE` to enable client-side CGO code generation for Go apps, `SRCLR_MAKE_WINDOWS` to preprocess C/C++ source with Make on Windows using a native gcc or clang compiler, and `--exclude` to prevent specified Java packages or JAR files from being scanned.

Package a C# project's source code directly for Static Analysis in a CI pipeline without a build step.

```
$ veracode package --csharp-source
```

— Six named flags/env vars each with exact purpose, one runnable example

CLI updates (2026-10-23)

02 Automated fix generation for SCA findings NEW 65

`veracode fix sca` generates fixes for vulnerable dependencies identified in SCA scans (Limited Availability), and now supports an asynchronous Fire-and-Forget (FnF) mode that submits remediation requests for background processing without waiting for fixes or pull requests to complete.

— Mechanism and availability stated but no runnable example CLI updates (2026-10-23)

03 Static scan and findings commands in CLI NEW 60

The CLI adds `veracode scan static` to run static scans and review security findings within a Git workflow, and `veracode findings static` to access cached static scan findings stored in the local Veracode directory.

Run a static scan on your Git repo and immediately review findings without leaving the command line.

```
$ veracode scan static
```

— Names both commands but little mechanism beyond purpose CLI updates (2026-10-23)

WAS THIS USEFUL? 👍 👎

◆ Software Supply Chain Security

Cycode

Feedback ⓘ

eMudhra Intermediate CA Compromise: What to Patch and How to Find It (2026-10-23)

BLOG ↗ RANK

Cycode's Agentic Development Security Platform unites security and development teams with actionable, code-to-runtime context to identify, prioritize, and fix the software risk that matters.

> Cycode shipped three new Threat Intelligence dashboard queries that surface where the compromised eMudhra intermediate CA trust still lingers across container images, runtimes, and Dockerfiles.

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

01 **Threat Intelligence dashboard queries for eMudhra CA exposure**

NEW 80

Adds three queries to the Threat Intelligence dashboard: Images with unpatched ca-certificates, which flags container images whose `ca-certificates` package is older than the fixed version for Alpine/Chainguard (apk), Debian/Ubuntu (deb), and RHEL/Fedora (rpm) packages, showing image tags and installed version; Images with outdated runtimes, which identifies images carrying Node.js, Java, pip, or certifi below the fixed versions that bundle their own trust data independently of the base image; and Dockerfiles on unpatched base images, which flags Dockerfiles built on Node.js, Python, Go, Java, Bun, or Deno images that are below the fixed version, on an end-of-life line, or pinned by digest. Each result links back to the originating repository, and the underlying Context Intelligence Graph queries also surface eMudhra CA exposure across dependencies, leaf certificates, CI/CD workflows, and developer machines.

⋮

Navigate to the Threat Intelligence dashboard to see how many of your assets contain unpatched ca-certificates, outdated runtimes, or Dockerfiles on unpatched base images, and open the underlying Context Intelligence Graph query for each.

> 📍 In Cycode, go to Threat Intelligence dashboard › view one of the three new items (Images with unpatched ca-certificates , Images with outdated runtimes , Dockerfiles on unpatched base images) › click the count to open the Context Intelligence Graph query and drill into affected repositories.

— Exact UI path given, but no API/CLI surface for automation

eMudhra Intermediate CA Compromise: Wha…

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Threat Intelligence

OpenCTI

Feedback ⓘ 7.261023.0 NOTES ↗ RANK

Open Cyber Threat Intelligence Platform

> OpenCTI 7.261023.0 focuses on knowledge graph usability, adding new export formats, keyboard control, object grouping, and filtering improvements, alongside ingestion health monitoring.

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

01 **Knowledge graph export, navigation and display improvements**

IMPROVED 40

The knowledge graph now supports SVG export and higher-resolution image export, keyboard stroke control for navigating graphs, grouping of objects of the same type together, and overall improved behavior for filtered items.

— Names concrete UI capabilities but no mechanism or exact controls given 7.261023.0

02 **Ingestion health monitoring** NEW 15

OpenCTI adds ingestion health monitoring, as referenced in the release summary, though no further detail on metrics or alerting is given.

— Mentioned only in summary with no detail on how it works 7.261023.0

WAS THIS USEFUL? 👍 👎

Flashpoint

Feedback ⓘ

Oct 22, 2026: Ransomware Files in Ignite (2026-10-22) BLOG ↗ RANK

Flashpoint empowers the world's leading organizations with the best data for threat intelligence to protect people, places, and assets.

> Flashpoint shipped Ransomware Files, a new searchable data type in Ignite that surfaces leaked file paths and directory trees from ransomware incidents with filtering, alerting, and API access.

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

01 **Ransomware Files data type in Ignite** NEW 88

Ignite adds Ransomware Files as a new searchable data type, letting users search leaked file trees from ransomware incidents by file name, path, or keyword to see exposure and directory structure before threat actors exploit it further. Results can be refined with filters for Ransomware Group, Victim Name, and File Type, and each result links directly to its originating ransomware victim post, which also gains a file sample view with one-click search for all related files from that leak. Users can set proactive alerts on critical file paths with real-time notifications delivered in-platform, via email, or to Slack channels, submit a Request for Intelligence (RFI) directly from a confirmed match, and pull Ransomware Files data programmatically through Flashpoint's Model Context Protocol (MCP) server for ingestion into SIEMs, SOARs, and internal tools.

Verify whether your organization's files appear in any ransomware leak, narrowing results to a specific threat group and file type.

📍 In Ignite, select the Ransomware Files data type › enter a file name or path keyword › apply filters: Ransomware Group = <group name>, File Type = <extension> › review results and click any result to open the originating victim post.

Automate monitoring of a sensitive file path so your team is instantly notified the moment it appears in a new leak.

📍 In Ignite, open Ransomware Files › run a search for the sensitive path › click Set Alert › configure notification channels: in-platform, email, and/or Slack channel › save the alert.

— Names filters, MCP server, Slack alerting, and gives UI navigation steps.

Oct 22, 2026: Ransomware Files in Ignit…

WAS THIS USEFUL?  

◆ SIEM

Databricks

Feedback ⓘ

Files API 3.0 for Unity Catalog volumes is now in Beta (2026-10-23) BLOG ↗

RANK

Databricks is a cloud-based data lakehouse platform for data engineering, analytics, machine learning, and AI workloads, built on Apache Spark.

> Databricks shipped Files API 3.0 multipart uploads and conditional operations for Unity Catalog volumes, a new Google Analytics Aggregated connector in Lakeflow Connect, a round of AI/BI dashboard upgrades including bulk Power BI/Tableau import and private bookmarks, and Beta support for configuring serverless job and bundle compute environments from pyproject.toml.

└──▷ WHAT SHIPPED · 7 FEATURES most completely described first ? what's the number?

01 Google Analytics Aggregated connector in Lakeflow Connect

NEW 78

Lakeflow Connect adds a managed Google Analytics Aggregated connector (Beta) for incremental ingestion of Google Analytics 4 report data — user activity, acquisition, engagement, monetization, demographics, and tech reports. It supports custom report definitions with user-defined dimensions, metrics, and aggregation level, and both service account and OAuth user-to-machine (U2M) authentication; workspace admins enable it from the Previews page.

Enable the Google Analytics Aggregated connector Beta for your workspace before configuring ingestion pipelines.

> 📍 In the Databricks workspace, go to Settings › Previews, find the Google Analytics Aggregated connector, and toggle it on.

— Clear enable path and auth/report scope named, no API payload shown

Google Analytics Aggregated connector i…

02 Bulk import of Power BI and Tableau files via Genie Code NEW

75

AI/BI dashboards support bulk import through Genie Code, bringing up to 100 Power BI (`.pbix`) or Tableau (`.twbx` / `.twb`) files at a time and converting them into AI/BI dashboards and metric views, rather than importing one file at a time.

Migrate a large Power BI or Tableau workspace to Databricks AI/BI dashboards all at once rather than one file at a time.

> 📍 In the Databricks UI, open Genie Code, select `Import multiple files in bulk`, and upload up to 100 Power BI (.pbix) or Tableau (.twbx/.twb) files to convert them to AI/BI dashboards and metric views.

– Exact UI steps, file formats, and 100-file limit given

Dashboard enhancements (2026-10-22)

---

03 **Serverless job environments configured via pyproject.toml**

NEW

70

Serverless notebook and Python script job tasks can read dependencies from a `pyproject.toml` file to configure their environment, configurable via the Jobs UI, Jobs API, or a bundle. Workspace admins enable this by turning on Project-Scoped Shared Compute on the Previews page.

Enable Project-Scoped Shared Compute so serverless job tasks can pick up dependencies from a `pyproject.toml` file.

> 📍 In the Databricks workspace, go to Settings › Previews and enable `Project-Scoped Shared Compute`.

– Enable path and config file named, but no API payload example

Serverless job environments from pyproj…

THINNER COVERAGE BELOW

04 **Files API 3.0 multipart uploads and conditional operations**

NEW

57

Files API 3.0 (Beta) adds multipart upload support for files larger than 5 GB to Unity Catalog volumes, and adds conditional operations that let upload, download, and delete act based on a file's current version to prevent unintended changes.

– Concrete 5GB limit and mechanism, but no endpoint or usage steps given

Files API 3.0 for Unity Catalog volumes…

---

05 **Private bookmarks for dashboard filter combinations** NEW

55

Dashboard viewers can save private bookmarks that preserve a filter combination and are visible only to themselves, letting them return to a saved view without affecting other users' dashboards.

Let analysts return quickly to a frequently used filter state without affecting other users' dashboard views.

📍 While viewing a dashboard, apply the desired filters, open the bookmarks menu, and select Save a private bookmark — the saved filter combination is visible only to your account.

— UI path given but no config or API surface named Dashboard enhancements (2026-10-22)

06 **Shared serverless compute for Asset Bundles** NEW 53

Databricks Asset Bundles can share serverless compute across tasks via a bundle-root `pyproject.toml` environment definition (Beta), enabled by turning on Project-Scoped Shared Compute on the Previews page.

Activate Project-Scoped Shared Compute so your workspace can use Shared Serverless for Asset Bundles.

📍 1. In your Databricks workspace, go to Settings › Previews. 2. Locate Project-Scoped Shared Compute and toggle it on.

— Thin description beyond the enable toggle and config file name

Shared Serverless for Asset Bundles (Be…

07 **Combo chart layering, waterfall totals, and field tooltips**

NEW 38

AI/BI dashboards add layered combo charts so authors can build combo charts from separate chart layers, customizable totals on waterfall charts, and full-name tooltips when hovering over a field or measure name in the field picker.

.

— Three thin UI additions with no steps or config named

Dashboard enhancements (2026-10-22)

UPDATED INTEGRATION Genie Ontology external tool query snippet extraction

> Genie One enhancements (2026-10-22) BLOG ↗ STABLE
>
> Genie One adds a conversation outline for navigation, skill-file uploads, and mobile email prefill.
>
> Adds Upload skills button to upload existing skill files and folders directly to your skills folder in the workspace (Public Preview).
>
> Adds conversation outline along the left edge of Genie One conversations to jump between messages and hover-preview responses.
>
> The Genie mobile app now remembers and prefills the last signed-in email address at next sign-in (Public Preview).

WAS THIS USEFUL? 👍 👎

Elastic Security Labs Feedback ⓘ

How CVE-2026-73570 turns a Zimbra log file into remote code execution (2026-10-23)

BLOG ↗ RANK

Elastic security labs is a powered by Elasticsearch. Ready to deploy your data?

> Elastic Security Labs shipped a new SIEM detection rule targeting active exploitation of the Zimbra Swatchdog command injection vulnerability (CVE-2026-73570).

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

01 **Zimbra Swatchdog command injection detection rule** NEW

85

Adds the Zimbra Swatchdog SNMP Command Injection Execution SIEM rule, which fires on a two-step process sequence: a shell spawned from a Perl `swatchdog_script` parent with `snmptrap`, `zmservicename`, and `zmservicestatus` in its command line, followed by any child process other than `snmptrap`. The rule can be enabled via Rules > Detection Rules in Elastic Security to alert on active exploitation and retroactively hunt for pre-patch attempts.

⋮

Enable the new Zimbra Swatchdog detection rule in Elastic Security to alert on active exploitation and hunt retroactively for pre-patch attempts.

📍 In Elastic Security, go to Rules › Detection Rules, search for Zimbra Swatchdog SNMP Command Injection Execution, and click Enable.

— Names exact rule, process chain fields, and enablement steps.

How CVE-2026-73570 turns a Zimbra log f…

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Vulnerability Management

vulnerability-db

Feedback ⓘ v7.0.3 NOTES ↗ RANK

Vulnerability database and package search for sources such as Linux, OSV, NVD, GitHub and npm. Powered by sqlite, CVE 5.2, purl, and vers.

> vulnerability-db v7.0.3 adds three new upstream advisory sources with an opt-out flag, verifies database image downloads layer-by-layer to prevent truncated files, and changes the purl spelling used for PHP and Node.js interpreter/runtime CVEs.

└──▷ **WHAT SHIPPED · 4 FEATURES** most completely described first ? what's the number?

01 **Bottlerocket, Oracle Linux and Seal Security advisory sources**

NEW 74

Adds ingestion of Bottlerocket (BRSA), Oracle Linux (ELSA), and Seal Security advisories as three new upstream advisory sources. Set `VDB_IGNORE_SEAL=true` to exclude the two Seal Security (`vulnfeed.sealsecurity.io`) OSV feeds from ingestion.

Exclude Seal Security feeds when building or refreshing a database in environments where only upstream package advisories are trusted.

```
$ VDB_IGNORE_SEAL=true vdb db refresh full
```

— Names sources, feed host and exact env var with runnable example v7.0.3

02 **PHP interpreter purl spelling change** BREAKING 65

The PHP interpreter is now stored as `pkg:generic/php` instead of `pkg:composer/php` ; databases built from this code no longer return interpreter CVEs under the old `pkg:composer/php` spelling.

— Exact before/after purl given but only a migration note v7.0.3

03 **Node.js runtime purl spelling change** BREAKING 65

Node.js runtime is now stored as `pkg:generic/nodejs/node` instead of `pkg:npm/node.js` and `pkg:npm/node` ; databases built from this code no longer return runtime CVEs under the old npm spellings.

— Exact before/after purl given but only a migration note v7.0.3

THINNER COVERAGE BELOW

04 Layer-by-layer verified database downloads IMPROVED

53

Image downloads now stream through a registry client that checks each layer's digest and size before moving the file into place, logging progress every GiB, so an interrupted download no longer leaves a truncated database.

— Mechanism described but no flag or command to act on `v7.0.3`

└──▷ **BREAKING ON UPGRADE**

! The PHP interpreter is stored as `pkg:generic/php` instead of `pkg:composer/php`; databases built from this code no longer return interpreter CVEs under the old `pkg:composer/php` spelling.

! Node.js runtime is stored as `pkg:generic/nodejs/node` instead of `pkg:npm/node.js` and `pkg:npm/node`; databases built from this code no longer return runtime CVEs under the old npm spellings.

WAS THIS USEFUL? 👍 👎

◆ Endpoint Management (UEM/RMM)

Iru Feedback ⓘ What's New in Iru | October 23rd NOTES ↗

Iru is a device-centric platform that unifies security, IT, and compliance around devices and everything they touch.

Iru gains automated FileVault key rotation and minimum OS enforcement in ADE, alongside AI-assisted policy library authoring.

Enables automatic FileVault key rotation triggered by Iru.

Adds minimum OS version enforcement within Automated Device Enrollment (ADE).

NEW SUPPORTED PLATFORM BitLocker and Android Restrictions Library Items with AI integration

WAS THIS USEFUL? 👍 👎

◆ Attack Surface & Exposure Management

runZero

Feedback ⓘ runZero 5.1.261022.0 (2026-10-22) BLOG ↗

An asset discovery and inventory platform that identifies and maps all devices on networks without requiring agents.

Broad search operator expansion across inventories: `notification_count:` numerics, `AND` / `OR` / `NOT` for scan templates and external reports, case-insensitive `domain:` matching, and tag editing on the Vulnerability details page.

Alert channel searches now support `notification_count:` with numeric comparisons such as `notification_count:>5`, and `settings:` now matches a channel's email recipients.

Scan template searches now support `AND`, `OR`, and `NOT` operators; a plain word searches template names and descriptions, and an unsupported keyword is reported as an error.

External report searches now support `AND`, `OR`, and `NOT` operators.

The `domain:` search is now case-insensitive in the asset, service, software, and vulnerability inventories, and an exact match such as `domain:=corp.example.com` finds assets that have that domain among others.

The searches `product:=` and `domain:=` now match assets with no products or no domains in the asset, service, software, and vulnerability inventories.

+2 more

UPDATED INTEGRATION Fingerprint improvements for FUJIFILM, Fortinet, DTEN, and printer device types in Azure AD integration

UPDATED SUPPORTED PLATFORM IBM OS/400 device detection resilience improvement

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Ping Identity

Feedback ⓘ 22 Oct 2026 (2026-10-23) BLOG ↗

RANK

Ping Identity is an identity and access management platform providing authentication, single sign-on, multi-factor authentication, and identity governance services.

> Ping Identity's AIC rapid channel adds QR-code rendering in scripted authentication nodes, multi-provider SAML import by alias, and OAuth/OIDC issuer-verification support, alongside a breaking change that normalizes managed object enum values to schema-defined case.

└──▷ **WHAT SHIPPED · 8 FEATURES** most completely described first ? what's the number?

01 **QR-code callback for scripted nodes** NEW 75

Adds callbacksBuilder.qrCodeCallback() binding to scripted nodes, enabling QR codes to render in the Advanced Identity Cloud admin console.

Generate a QR code inside a scripted authentication node to display to users in the admin console.

```
$ callbacksBuilder.qrCodeCallback()
```

— Names exact API call and shows runnable usage example. 22 Oct 2026 (2026-10-23)

02 **(improved) OAuth2/OIDC authorization flow enhancements**

IMPROVED 75

Authorization code requests (including PAR) can now omit the `scope` parameter when `authorization_details` are requested with Rich Authorization Requests and RCS enabled, and the OpenID Connect discovery endpoint now always returns `authorization_response_iss_parameter_supported: true` while authorization responses (including error responses) that redirect to the client include the `iss` parameter for issuer verification.

— Names exact parameters and request types involved. Names exact discovery field and response parameter added.

22 Oct 2026 (2026-10-23)

03 **Managed object enum case normalization** BREAKING 70

Managed object enum values are now rewritten to the exact schema-defined case on create, update, or patch (e.g. `Active` becomes `active` if the schema defines `active`).

Scripts or dashboards that compare enum property values using non-schema case will need to be updated to expect the schema-defined case.

— Gives before/after example and clear migration note. 22 Oct 2026 (2026-10-23)

04 **Multi-provider SAML import by alias** NEW 60

Adds support for importing multiple remote identity providers that share the same entity ID by specifying an alias; alias uniqueness is enforced per circle of trust.

— Explains mechanism but no exact config field or command shown. 22 Oct 2026 (2026-10-23)

THINNER COVERAGE BELOW

05 **Custom reports field and parameter flexibility** IMPROVED 55

In custom reports, the Completed By field in the Entitlement Review Item entity now returns the `userName` value, and several parameters in built-in reports are now optional, allowing reports to be run with broader criteria.

— Names specific field and entity but lacks full parameter list. 22 Oct 2026 (2026-10-23)

06 **Custom name formats for WS-Fed attributes** IMPROVED 45

Custom WS-Fed applications now support user-defined name formats for service provider attributes, allowing custom namespaces for relying party compatibility.

— Describes benefit but no concrete config path given. 22 Oct 2026 (2026-10-23)

07 **Unique username and application name enforcement** IMPROVED 30

The underlying datastore now enforces unique usernames and application names.

— Bare statement with no mechanism or scope detail. 22 Oct 2026 (2026-10-23)

08 **Certificate node security hardening** IMPROVED 30

Version 2 of the Certificate Collector and Certificate Validation nodes includes security hardening improvements.

— Names the nodes but gives no detail on what hardening changed. 22 Oct 2026 (2026-10-23)

└──▷ BREAKING ON UPGRADE

! Managed object enum values are now rewritten to the exact schema-defined case on create, update, or patch (e.g. `Active` becomes `active` if the schema defines `active`). Scripts or dashboards that compare enum property values using non-schema case will need to be updated to expect the schema-defined case.

WAS THIS USEFUL?

Clerk

Feedback ⓘ Agent feedback (2026-10-23) BLOG ↗ RANK

Clerk is an authentication and user-management platform that provides pre-built UI components, APIs, and SDKs for adding sign-up, sign-in, and identity features to applications.

> Clerk shipped two distinct capabilities this window: AI agent feedback submission via an MCP server, and a Backend API endpoint for merging duplicate user accounts.

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

01 **Agent feedback submission via MCP server** NEW 35

AI agents can submit product feedback directly from an MCP server, with submissions reviewable in the Clerk dashboard.

— Describes mechanism but no endpoint, flag, or config name given

Agent feedback (2026-10-23)

02 **Merge duplicate users via Backend API** NEW 35

A new Backend API endpoint merges a duplicate user into another user and deletes the duplicate.

— Names the capability but not the exact endpoint path or method

Merge two users into one (2026-10-23)

WAS THIS USEFUL?

1Password

Feedback ⓘ 1Password CLI Beta 2.43.0-beta.02 (2026-10-22)

BLOG ↗ RANK

All the latest releases from the 1Password team

> 1Password's CLI beta improves secret listing for 1Password Environments with a new export format and richer output.

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

01 Dotenv export and richer output for environment secrets

IMPROVED 80

The `op environment secret list` command gains `dotenv` as a new option for the `--format` flag, letting users export all secrets in a 1Password Environment as a dotenv file (e.g. `op environment secret list --format dotenv > .env`). The command's output now also displays the name, value, and concealment status of each secret.

Export all secrets in a 1Password Environment as a dotenv file for use in local dev tooling or CI pipelines.

```
$ op environment secret list --format dotenv > .env
```

— Names exact command, flag and new format with runnable example

1Password CLI Beta 2.43.0-beta.02 (2026…

WAS THIS USEFUL? 👍 👎

◆ Data Security & DLP

Varonis

Feedback ⓘ Create new automations with cloning NOTES ↗

RANK

Varonis is the leading data and AI security platform that proactively reduces risk, enforces policies, and stops active threats with our AI-native automation.

> Varonis rolled out automation cloning, expanded Exact Data Match to tabular files with offline preparation for air-gapped networks, added CSV output and a folder-to-entity-ID lookup API for its Export/Search APIs, plus a unified classification pattern workspace and reusable data source collections.

└──▷ **WHAT SHIPPED · 7 FEATURES** most completely described first ? what's the number?

01 **Entity ID Lookup API for folder paths** NEW 80

A new Entity ID Lookup API resolves physical folder paths into the entity IDs required by the Search and Export APIs, supporting exact path resolution, bulk lookups, path discovery, and subtree resolution.

– Names API and its modes but no endpoint signature given

Resolve data entity IDs directly from f…

02 **Offline EDM source data preparation** NEW 65

EDM source data can now be hashed on disconnected systems and only the hashed package uploaded from a connected environment, keeping source data within restricted or air-gapped networks.

– Mechanism clear but no exact command or config key

Expand Exact Data match coverage and pr…

03 **CSV output for Export API** IMPROVED 60

The Export API now supports native CSV output in addition to the existing AVRO format, eliminating conversion steps for spreadsheet and reporting workflows.

– Names the API and formats but no sample call shown Export API results in CSV format

THINNER COVERAGE BELOW

04 **Exact Data Match coverage for tabular files** IMPROVED

55

Exact Data Match (EDM) classification now extends to tabular files, enabling the same policies to apply across both tabular and non-tabular data.

— Explains scope change but no concrete UI/API steps

Expand Exact Data match coverage and pr…

05 **Clone existing data protection automations** NEW

50

Automations can now be cloned to reuse an existing configuration instead of rebuilding it from scratch, supporting consistent policy deployment across environments. In the Varonis console, navigate to an existing automation, select Clone, adjust environment-specific settings on the copy, then save and deploy.

When you need to roll out a consistent automation policy across multiple environments without manually recreating each configuration.

> 📍 In the Varonis console, navigate to your existing data protection automation, select Clone, adjust environment-specific settings on the copy, then save and deploy.

— UI path given but no named config fields or API Create new automations with cloning

06 **In-app classification pattern workspace** NEW

50

A unified classification pattern workspace in the Varonis Web Interface lets users create, edit, test, and manage classification patterns without switching tools.

— Names the surface but no exact navigation path Manage classification patterns from a s…

07 **Reusable named data source collections** NEW

45

Multiple data sources can be grouped into named collections that are reusable across analytics, dashboards, and policies, reducing repetitive source selection.

— Describes capability but no UI steps or config detail

Organize data sources into reusable col…

UPDATED INTEGRATION SharePoint Online and OneDrive Main links monitoring

Monitor Microsoft Main links in SharePoint and OneDrive NOTES ↗ STABLE

WAS THIS USEFUL? 👍 👎

◆ Integrated & IT Risk Management

CISO Assistant

Feedback ⓘ v4.1.4 NOTES ↗

CISO Assistant is a one-stop-shop GRC platform for Risk Management, AppSec, Compliance & Audit, TPRM, BIA, Privacy, and Reporting. It supports 200+ global frameworks with automatic control mapping, including ISO 27001, NIST CSF, SOC 2, CIS, PCI DSS, NIS2, DORA, GDPR, HIPAA, CMMC, and more.

v4.1.4 adds MCP tools for folders/users/evidence, DPIA import from CNIL PIA, a dynamic data wizard, solutions tiering, expanded labels, and persistent Helm file storage.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v4.1.4 https://github.com/intuitem/ciso-assistant-community.git
# already have the repo? check out this version:
$ git checkout v4.1.4
```

Adds `update_folder`, `update_user`, and `update_evidence` tools to the MCP integration.

Supports importing DPIA studies from CNIL's PIA tool exports into the privacy module.

Adds dynamic data wizard with headers and fields mapping in the epic import flow.

Surfaces questionnaire compliance scores on entity assessments in the TPRM module.

Expands label support to more object types and introduces a dedicated view listing all objects associated with a label.

+5 more

NEW COMPLIANCE FRAMEWORK ISO/IEC 27090:2026 outline

NEW COMPLIANCE FRAMEWORK R-CNMV-2024-08-MV Dominican Republic securities market cybersecurity regulation

UPDATED INTEGRATION n8n custom node restructured

NEW INTEGRATION Microsoft Graph mail transport

NEW SUPPORTED PLATFORM Hungarian translation

WAS THIS USEFUL? 👍 👎

AGENT

◆ MCP Servers & Tooling

Runlayer

Feedback ⓘ 1.35.0 (2026-10-23) BLOG ↗ RANK

Runlayer is an MCP gateway that enforces identity-mapped permissions and detects threats across the agents and MCP servers employees use.

> Runlayer's 1.35.0 release adds bulk deletion of disabled agents, read-only .xlsx spreadsheet previews in the artifact viewer, and automatic publishing of agent-created files to Artifacts, alongside MDM policy details for the Chrome extension and several smaller UI clarifications.

└──▷ **WHAT SHIPPED · 8 FEATURES** most completely described first ? what's the number?

01 **Bulk deletion of disabled agents** NEW 75

From the Agents Inventory tab, admins can select multiple disabled agents and choose Delete to remove them in one action, including their schedules, webhooks, and Slack apps; enabled agents are left untouched.

Clean up a large fleet of decommissioned agents — including their schedules, webhooks, and Slack apps — in a single action rather than one at a time.

📍 In the Runlayer console, go to Agents → Inventory tab, check the disabled agents you want to remove, then choose Delete from the bulk-action menu.

— Exact UI path and mechanism given, scope limited to disabled agents.

1.35.0 (2026-10-23)

02 **Read-only .xlsx previews in artifact viewer** NEW 70

Agents' Excel outputs can now be previewed directly in the artifact viewer without downloading, with a tab per sheet and preservation of the workbook's number formats, colors, and merged cells.

— Names format and preserved attributes but no command or exact navigation.

1.35.0 (2026-10-23)

THINNER COVERAGE BELOW

03 **Automatic publishing of agent-created files to Artifacts**

IMPROVED 55

Agents now automatically publish files they create — decks, documents, spreadsheets, PDFs — to Artifacts and reply with a link, instead of reporting that there is no way to share them.

— Clear before/after behavior with named file types but no exact command.

1.35.0 (2026-10-23)

04 **Compliance import scope clarification** IMPROVED 45

In Settings → Agent session monitoring, the UI now clarifies that a Claude or ChatGPT compliance import covers every user in the connected organization or workspace, including people who have never signed in to Runlayer.

— Documentation-only clarification with exact UI location but no new mechanism.

1.35.0 (2026-10-23)

05 **Shared environment variable tooltips on connectors** IMPROVED 30

Tooltips on hosted connectors' shared environment variables now explain whether a value is shared across all users or entered individually per user.

— Explains the clarification but no actionable surface named. 1.35.0 (2026-10-23)

06 **Access tooltips on shared agents** IMPROVED 30

Tooltips on shared agents now describe what access level the viewer holds and who to ask for Can edit permission when a trigger, scheduled task, or connector cannot be added.

— Clear description of the UI clarification but no concrete action path.

1.35.0 (2026-10-23)

07 **Skip all setup checklist steps at once** IMPROVED 25

Admins can now skip all remaining setup checklist steps in a single action instead of dismissing them one by one.

— Minor admin convenience with no further detail. 1.35.0 (2026-10-23)

08 **Emoji agent faces as Slack app icons** IMPROVED 20

An agent whose face is an emoji now displays that emoji as its Slack app icon instead of the default Runlayer logo.

— Bare description of a cosmetic change. 1.35.0 (2026-10-23)

WAS THIS USEFUL? 👍 👎

DEPLOY

◆ Agentic Infrastructure

microsandbox Feedback ⓘ v0.7.10 NOTES ↗ RANK

easy, fast, programmable and local-first microVM runtime and library

> microsandbox v0.7.10 adds anonymous registry authentication to the Go SDK, allowing image pulls from OCI registries that don't require credentials.

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

01 **Anonymous registry auth in Go SDK** NEW 40

The Go SDK now supports anonymous registry authentication, enabling pulls from OCI registries that do not require credentials.

— Names SDK and auth type but no method, flag, or config shown. v0.7.10

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI Runtime Defense & Guardrails

Operant AI

Feedback ⓘ

The Season of Agentic Commerce is Here, Are You Ready? NOTES ↗ RANK

Operant AI discovers, detects and defends AI applications, agents, MCP servers, APIs and Kubernetes workloads at runtime.

> Operant AI launched Agentic Commerce Defense, a new runtime protection layer that detects and blocks malicious AI shopping agents at checkout while distinguishing them from legitimate ones.

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

01 **Agentic Commerce Defense for AI shopping agents** NEW

62

A new runtime protection layer distinguishes legitimate shopping agents (e.g., Meta Muse, OpenAI Dots) from scalper fleets, scrapers, and rogue agents at checkout. It includes loop detection that identifies a paid API call repeating without progress to stop runaway token and dollar spend from misbehaving pricing or merchandising agents, per-agent token limits that throttle a single misbehaving agent independently without affecting other agent instances, and runtime behavioral analysis that tracks agent activity across a full session to identify coordinated fleet behavior distinct from a single genuine shopper's intent.

— Mechanism described well but no config/flags or setup steps given.

The Season of Agentic Commerce is Here,…

WAS THIS USEFUL? 👍 👎

◆ AI Red Teaming & Testing

clawscan

Feedback ⓘ v0.3.0 NOTES ↗ RANK

Composable security scanning harness for agent skills

> clawscan v0.3.0 adds opt-in lifecycle diagnostics for scan phases, introduces a breaking v2 schema for versioned judge inspection receipts with live Ubuntu verification, and hardens its build and runtime supply chain against compromised certificates and unsafe overwrites.

└──▷ **WHAT SHIPPED · 7 FEATURES** most completely described first ? what's the number?

01 Versioned judge inspection receipts and verification BREAKING

65

Binds versioned judge inspection receipts (schema version 2) to required-file hashes and canonical inspected paths, retrying invalid inspection once within the original deadline. Also adds an opt-in live judge inspection check on Ubuntu 22.04 that verifies package-file receipts without publishing. Consumers validating receipt keys must accept the version 2 schema.

– Names schema version and OS but no migration command v0.3.0

THINNER COVERAGE BELOW

02 Opt-in lifecycle diagnostics for scan phases NEW

45

Adds opt-in phase and bounded child-judge lifecycle diagnostics that survive outer scan interruption without exposing commands, paths, or raw output.

– Describes behavior but no flag or command named to enable it v0.3.0

03 Resilient retry for A.I.G stream overload IMPROVED

45

Retries transient `A.I.G` stream overload within the original deadline and finishes cleanup before returning caller interrupts.

– Explains retry behavior but gives no config or API v0.3.0

04 Hardened Claude runtime certificate and Node pinning IMPROVED

45

Updates the bundled Claude runtime to reject compromised certificate-authority keys and pin Node releases with incident-key rejection.

– Names mechanism but no version numbers or config key v0.3.0

05 **Cancellation evidence and input protection safeguards**

IMPROVED 40

Preserves cancellation and preparation evidence, rejects unsafe output aliases, and protects scan inputs and loaded configuration from overwrite.

— Describes safeguards but names no flags or files v0.3.0

06 **Runtime images published from verified native builds** IMPROVED

25

Publishes runtime images only from verified native platform builds.

— Single sentence with no mechanism or named artifact v0.3.0

07 **Parallelized SkillSpector discovery** IMPROVED 25

Parallelizes SkillSpector discovery as part of the scan harness, per the release summary.

— Only mentioned in summary, no further detail given v0.3.0

└──▷ **BREAKING ON UPGRADE**

! Consumers validating receipt keys must accept the version 2 schema for versioned judge inspection receipts.

WAS THIS USEFUL?  

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

OpenSSL

Feedback ⓘ openssl-4.1.0 NOTES ↗ CODE ↗ RANK

General purpose TLS and crypto library

> OpenSSL 4.1.0 adds DTLS 1.3 and GREASE support alongside post-quantum crypto performance optimizations, while removing several legacy Configure options and build targets.

└──▷ **WHAT SHIPPED · 9 FEATURES** most completely described first ? what's the number?

01 **no-ec replaces no-ecdsa and no-ecdh** BREAKING 70

The `no-ecdsa` and `no-ecdh` Configure options are removed; use `no-ec` to disable elliptic curve support instead.

— Exact flags named with clear migration instruction openssl-4.1.0

02 **tsget now requires Net::Curl::Easy** BREAKING 70

The `tsget` utility now requires `Net::Curl::Easy` (from the Net-Curl CPAN distribution) instead of the abandoned `WWW::Curl::Easy` — install it before upgrading.

— Exact dependency and upgrade action named openssl-4.1.0

THINNER COVERAGE BELOW

03 **MSVC 2013 build targets** NEW 55

Adds `VC-WIN32-MSVC2013` and `VC-WIN64A-MSVC2013` build targets for MSVC 2013 C99 bridging support.

— Exact target names given, directly usable in Configure openssl-4.1.0

04 **Post-quantum crypto performance optimizations** IMPROVED 50

Adds optimized ML-DSA and ML-KEM NTT operations on `ppc64le`, and optimized ML-DSA operations on `x86_64` including AVX-512-optimized SHAKE x4 for ML-DSA and AVX-512/VAES optimizations for AES-CBC decryption.

— Specific algorithms and architectures named, no enablement steps given openssl-4.1.0

05 **DTLS 1.3 protocol support** NEW 45

Adds DTLS 1.3 support per RFC 9147, documented in the ossl-guide-dtlsv13(7) manual page; the release also introduces a new DTLS listener API.

— Names RFC and manual page but no usage mechanism given `openssl-4.1.0`

06 **VC-WIN64I and VC-CE build targets dropped** BREAKING 45

The `VC-WIN64I` (Windows-on-Itanium) and `VC-CE` (Windows CE) build targets are dropped from Configurations.

— Exact removed targets named, no replacement path given `openssl-4.1.0`

07 **GREASE extension support** NEW 30

Adds RFC 8701 GREASE (Generate Random Extensions And Sustain Extensibility) support.

— Named standard but no behavioural or config detail `openssl-4.1.0`

08 **Elbrus2000 (e2k) architecture support** NEW 30

Adds initial support for the Elbrus2000 (`e2k`) architecture.

— Bare name of new architecture support, no further detail `openssl-4.1.0`

09 **IKEV2 KDF support** NEW 15

Adds IKEV2 KDF support, per the release summary; no further implementation detail provided.

— Only named in summary with no further detail `openssl-4.1.0`

└──▷ **BREAKING ON UPGRADE**

! The `no-ecdsa` and `no-ecdh` Configure options are removed; use `no-ec` to disable elliptic curve support.

! The `tsget` utility now requires `Net::Curl::Easy` (from the Net-Curl CPAN distribution) instead of the abandoned `WWW::Curl::Easy` — install it before upgrading.

! The `VC-WIN64I` (Windows-on-Itanium) and `VC-CE` (Windows CE) build targets are dropped from Configurations.

WAS THIS USEFUL? 👍 👎

OTHER / UNCATEGORIZED

◆ UNCATEGORIZED

ArmorCode

Feedback ⓘ announced · Oct 24, 2026 BLOG ↗ RANK

ArmorCode is the independent control plane where AI agents help find, prioritize, and fix vulnerabilities across apps, cloud, infra, and AI.

> ArmorCode launched ArmorCode Zero, a new agentic remediation product that auto-triages and groups vulnerability findings into fixable changes, drafts pull requests, and verifies closure via rescan, backed by a conversational interface and a new Context Risk Graph knowledge layer.

└──▷ **WHAT SHIPPED · 4 FEATURES** most completely described first ? what's the number?

01 **ArmorCode Zero agentic remediation engine** NEW 64

ArmorCode Zero reads every finding, automatically writes a triage call, and groups findings by the single change that resolves them, then drafts pull requests and proves closure via rescan. In ArmorCode's own testing this reduced a backlog of roughly 28,600 findings to about 8,900 fixes, a 69% reduction.

— Mechanism and concrete before/after numbers given, but no command or config surface.

launch-20261024-b7bae079

THINNER COVERAGE BELOW

02 **Context Risk Graph knowledge layer** NEW 47

The ArmorCode Context Risk Graph is a shared knowledge layer that connects findings to assets, code, owners, business services, and controls, enabling risk-ranked fix prioritization.

— Names the graph and what it links, but no interface or query detail.

launch-20261024-b7bae079

03 **Conversational interface for security data** NEW 36

Zero adds a conversational interface where security teams can ask questions, request charts, and describe trends in plain language, with charts and flows built on demand from the team's own data.

— Describes the capability but no named commands or exact navigation.

launch-20261024-b7bae079

04 **Secret redaction and bring-your-own model keys** NEW 36

ArmorCode Zero redacts secrets before any model call and supports bring-your-own model keys for teams using their own AI providers.

— States the safeguard and option but no configuration details given.

launch-20261024-b7bae079

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · October 24, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue