THE CYBER TOOLCHAIN

NO. 059

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED AUGUST 30, 2026 · EVERY DAY

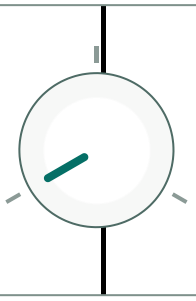
The daily firehose — everything the toolchain shipped today, already filtered.

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // **CONTENTS** SHOW 7 tools

OFFENSIVE SECURITY

vim ? help

◆ Post-Exploitation

chisel

Feedback ⓘ 1 RELEASE · 2026-08-29 NOTES ↗

A fast TCP/UDP tunnel over HTTP

> Chisel 1.12 tightens SOCKS5 and authentication security with several breaking changes, while adding configurable retry backoff, socks5:// client proxying, graceful shutdown, and multi-arch container images.

└──▷ WHAT SHIPPED · 13 FEATURES most completely described first ? what's the number?

01 SOCKS5 access now requires explicit authfile ACL entry

80

BREAKING

With `--socks5` and `--authfile`, users who need SOCKS5 access must now have an authfile entry matching `socks`; previously SOCKS5 bypassed the ACL list entirely. The wildcard `""` continues to match everything including `socks`.

Update an authfile to explicitly permit a user SOCKS5 access after upgrading to 1.12, where SOCKS5 no longer bypasses ACLs.

json

```
{
  "foo:bar": ["^10\.0\.0\.1:80$", "socks"]
}
```

— Names exact ACL token and shows a migration example config v1.12.0

02 Configurable client retry backoff intervals NEW

70

Adds `--min-retry-interval` and `--max-retry-interval` flags to tune client exponential-backoff retry timing, letting operators slow reconnect attempts on unstable links.

Slow down retry attempts on an unstable link so the client waits longer between reconnects before hitting `--max-retry-count`.

```
$ chisel client --min-retry-interval 5s --max-retry-interval 60s
--max-retry-count 10 https://chisel.example.com
3000:localhost:3000
```

— Named flags plus a runnable example command v1.12.0

03 **Stricter --fingerprint format requirement** BREAKING 65

Requires `--fingerprint` to supply the full SHA256 fingerprint or the full 16-octet MD5 colon form; truncated MD5 prefixes are now rejected.

— Names flag and exact accepted formats v1.12.0

04 **Stricter --auth colon format requirement** BREAKING 60

Requires `--auth` values to use `<user>:<pass>` format with a colon; values without a colon now fail at startup instead of silently disabling authentication.

— Names flag and exact before/after failure behaviour v1.12.0

05 **Multi-arch scratch-based container images** NEW 60

Ships ko-built, scratch-based images with CA roots for six architectures, published to Docker Hub (`jpillora/chisel`) and GHCR (`ghcr.io/jpillora/chisel`).

— Names exact registries and image paths for pulling v1.12.0

THINNER COVERAGE BELOW

06 **Reliable authfile hot-reload across editors and Kubernetes** IMPROVED 55

Authfile reloads now work reliably across editor rename-on-save and Kubernetes ConfigMap swaps; ACL changes apply to new tunnels without interrupting established ones.

— Describes fix and behaviour but no reproduction steps v1.12.0

07 **Retry exhaustion now exits non-zero** BREAKING 50

A client that exhausts `--max-retry-count` now exits with a non-zero status code, making retry exhaustion detectable in scripts and CI.

— Names flag and exact new exit behaviour v1.12.0

08 **Graceful SIGTERM shutdown with request draining** NEW 50

Adds graceful SIGTERM shutdown with in-flight HTTP request draining so active tunnels complete cleanly before the process exits.

— Describes mechanism but no config or flag to invoke v1.12.0

09 **socks5:// proxy URL scheme for clients** NEW 45

Adds `socks5://` scheme support for client proxy URLs, enabling chisel clients to egress through a SOCKS5 proxy.

— Names the scheme but gives no example of use v1.12.0

10 **Pre-authentication WebSocket message capping** IMPROVED

40

Caps pre-authentication WebSocket messages while preserving every valid SSH packet, hardening the unauthenticated attack surface.

— Explains hardening but no tunable value or flag given v1.12.0

11 **Version reporting and session-event logging** IMPROVED

35

Reports accurate version strings for `go install` builds and adds info-level logs for session establishment, authentication events, and ACL denials.

— Names log categories but no format or flag detail v1.12.0

12 **Release archive integrity testing in CI** IMPROVED 35

Release CI now integrity-tests every `.gz` and `.zip` archive before any asset or image is published.

— Internal CI process, no user-facing action v1.12.0

13 **CLI parsing migrated to opts library** IMPROVED 25

Migrates CLI parsing and help output to `opts` with terminal-aware formatting and reliable wrapping at narrow widths.

— Bare mention of internal dependency swap v1.12.0

└──▷ **BREAKING ON UPGRADE**

! With `--socks5` and `--authfile`, users who need SOCKS5 access must have an authfile entry matching `socks`; SOCKS5 previously bypassed the ACL list entirely.

! `--fingerprint` now rejects truncated MD5 prefixes; only the full SHA256 fingerprint or the full deprecated 16-octet MD5 colon form is accepted.

! `--auth` values without a colon now cause startup failure instead of silently disabling authentication.

! A client that exhausts `--max-retry-count` exits non-zero; previously the exit code did not reliably signal retry exhaustion.

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ Web Application Security

humble

Feedback ⓘ 1 RELEASE · 2026-08-29 NOTES ↗

A humble and fast security-oriented HTTP headers analyzer.

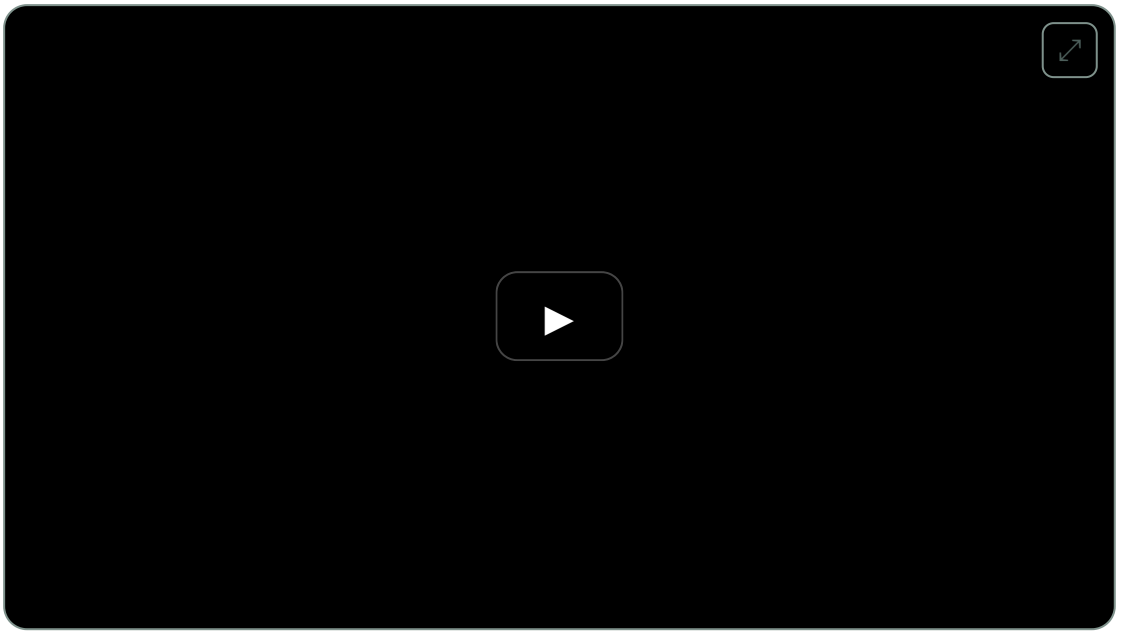
> humble 1.65 expands its HTTP header detection database with new fingerprinting signatures and an additional insecure-value check.

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

01 Expanded fingerprint and insecure header detection IMPROVED

50

Added 3 new fingerprint headers (commits `b83d699` and `732522f`) to the detection database, expanding coverage to identify server/framework exposure via HTTP response headers, and 1 new insecure value check (commit `3b59c53`), increasing the total number of insecure/deprecated header checks.



— Names commit hashes and counts but no flags or config. 1.65

WAS THIS USEFUL? 👍 👎

◆ SAST / SCA / Code Security

GitHub

Feedback ⓘ 2 RELEASES · 2026-08-28 BLOG ↗

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

> GitHub Copilot's biggest updates this window were in Visual Studio — org-level custom agents, a Git agent that reviews changes before a PR, and model management/thinking-effort controls — alongside a broad weekly Copilot refresh spanning a Rust-powered CLI, shared Slack/Teams agent sessions, a GA Customize tab with Azure DevOps integration, JetBrains enterprise controls, and VS Code 1.135 chat improvements.

└──▷ WHAT SHIPPED · 13 FEATURES most completely described first ? what's the number?

01 Git agent code review in Visual Studio Copilot NEW

80

The Git agent can review uncommitted changes or individual commits before a pull request is opened, with findings surfaced inline in the editor and a navigable list in Git Changes, for both GitHub and Azure DevOps repositories.

Use the Git agent to catch issues in uncommitted work before opening a pull request, without leaving Visual Studio.

> 📍 In the Copilot Chat pane, select the Git agent, then type: Review my uncommitted changes. Findings appear inline in the editor; navigate them via the list in Git Changes.

— Includes a runnable chat command and exact navigation path.

GitHub Copilot in Visual Studio — Augus… | GitHub Copilot weekly releases — August…

02 Model management and thinking effort controls in Visual Studio

NEW

75

Adds thinking effort controls — Low, Medium, and High — for supported models, letting you trade reasoning depth against token usage per task. Also adds model management: pin favorite models, collapse less-used ones, and open Manage models for a view of capabilities, context window sizes, cost information, and controls for Copilot and custom models.

Lower token consumption for a quick, routine edit by setting thinking effort to Low instead of the default.

📍 In the Copilot model picker, select your model, then choose `Low` under the thinking effort control before sending your prompt.

— Names exact effort levels and picker UI, with a runnable example.

GitHub Copilot in Visual Studio — Augus… | GitHub Copilot weekly releases — August…

---

03 **`defaultMode` and `defaultPermissionMode` in Copilot CLI** NEW

70

Adds `defaultMode` and `defaultPermissionMode` settings to GitHub Copilot CLI so every new session starts with your preferred execution and permission modes.

— Names exact config keys, ready to set. GitHub Copilot weekly releases — August…

---

04 **Plugin, MCP, and skills management in Copilot CLI** NEW

65

Adds new management experiences for plugins, MCP servers, and skills via `/plugin`, `/mcp`, and `/skills` commands in the Copilot CLI.

— Three named slash commands, directly runnable. GitHub Copilot weekly releases — August…

---

05 **Organization-level custom agents in Visual Studio Copilot**

NEW

60

Org and enterprise owners can publish custom agents that Visual Studio automatically detects, showing descriptions and organization source in the agent picker, enabling teams to share custom agents to standardize workflows.

— Explains publishing and detection but no exact setup steps.

GitHub Copilot in Visual Studio — Augus… | GitHub Copilot weekly releases — August…

---

06 **Customize tab GA with Azure DevOps integration** IMPROVED

60

The Customize tab in the GitHub Copilot app is now generally available, bringing MCP servers, plugins, skills, and canvases together in one place; it also adds Azure DevOps issue and pull request integration, enabling Copilot sessions to be started from ADO work items.

— Names the tab and ADO surface but not exact navigation steps.

GitHub Copilot weekly releases — August…

THINNER COVERAGE BELOW

---

07 **Shared agent sessions in Slack and Microsoft Teams** NEW

55

Introduces shared agent sessions in GitHub Copilot for Slack and Microsoft Teams — mention `@GitHub` to investigate problems, plan work, and make changes your whole

team can follow and guide together.

— Gives the exact mention trigger but no further detail.

GitHub Copilot weekly releases — August…

08 **Copilot usage and plan consumption view in Visual Studio** NEW 50

Adds View all Copilot usage in the context window (opened from the Copilot prompt box) to see full plan details and approaching-limit notifications, also described as a plan consumption view to monitor and manage premium model usage before hitting limits.

— UI location given but no deeper mechanism or numbers.

GitHub Copilot in Visual Studio — Augus… GitHub Copilot weekly releases — August…

09 **VS Code 1.135 Copilot chat improvements** IMPROVED 50

VS Code 1.135 lets you continue recent Copilot or Claude agent sessions started in other applications, adds a complementary-model second opinion mode to surface missed details and edge cases, adds per-turn per-model detailed chat usage breakdowns, and introduces a new single-pane Agents layout with simpler session controls.

— Four named features listed but no commands or config given.

GitHub Copilot weekly releases — August…

10 **WSL support and tab management in Copilot app** NEW 45

Adds experimental Windows Subsystem for Linux (WSL) support in the Copilot app, plus tab split-and-move and external browser preview via the tab context menu.

— Names the context menu path but marked experimental with little detail.

GitHub Copilot weekly releases — August…

11 **Enterprise controls for Copilot in JetBrains** NEW 45

Adds enterprise controls for GitHub Copilot in JetBrains, covering plugins, MCP servers, telemetry, and agent permission modes.

— Names four control areas but no configuration steps given.

GitHub Copilot weekly releases — August…

12 **Native Rust runtime for Copilot CLI** IMPROVED 40

Copilot CLI now runs on a native Rust runtime for significantly faster performance while keeping the terminal interface in TypeScript.

— States mechanism and outcome but nothing for reader to do.

GitHub Copilot weekly releases — August…

13 **Session restore in Copilot CLI** NEW 40

Adds session restore in Copilot CLI, letting you pick up sessions that did not exit cleanly, including those interrupted mid-turn.

— Describes behaviour but no command or flag given.

GitHub Copilot weekly releases — August…

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Network Analysis & Monitoring

SO-CRATES

Feedback ⓘ 4 RELEASES · 2026-08-04 → 2026-08-25 NOTES ↗

SO-CRATES: Security Onion Containerized Rapid Analysis of Threats, Evil, and Sus!

> SO-CRATES shipped four releases spanning new network-analysis heuristics (DNS tunneling/DGA scoring, community-ID correlation, JA3/JA4 TLS fingerprinting), an alert acknowledgment workflow with app-wide keyboard navigation and a command palette, AI-generated rule summaries and Security Onion Playbooks guidance, an in-UI Rules modal with automatic rule refresh, and per-row plus whole-analysis note-taking via new API endpoints.

└──▷ WHAT SHIPPED · 21 FEATURES most completely described first ? what's the number?

01 Rules modal for rule management and staleness NEW

93

A new Rules modal, accessible from the gear menu, shows each ruleset's current rule count, last-updated timestamp, and per-ruleset `Update` and `Update All` buttons — rule updates no longer block server startup. It surfaces upstream sources with links: Suricata to Emerging Threats Open, YARA to YARA Forge, Sigma to SigmaHQ. Ruleset `updated` dates are highlighted in warning color when more than 30 days old or never successfully updated, across all four rulesets (Suricata, YARA, Sigma Windows, Sigma Linux). Rule update progress shows a spinner and elapsed-time counter (`Updating... 45s`) with an on-demand `View Log` /'Hide Log' toggle for the raw update log, polled via `/api/rule-update-status`. A one-time sticky toast appears on first load when `/api/rules-info` shows no rules for all three engines, with a direct `Open Rules` link to the Rules modal.

Check whether all three rule engines have rules loaded before relying on detections, and surface the Rules modal link if any engine reports zero rules.

```
$ curl -s http://localhost:8000/api/rules-info | python3 -m json.tool
```

— Names every endpoint and threshold, with a runnable check command. v3.1.0

02 AI-generated rule summaries NEW

90

`AI_SUMMARIES_DIR` environment variable lets manual (non-Docker) installs point at a locally-built AI summary index for Suricata, Sigma, and YARA rule explanations. Expanding a Suricata alert, Sigma alert, or YARA file match now shows an AI Summary — a plain-English explanation of what the rule detects — sourced from Security Onion's

`securityonion-resources` repository (`generated-summaries-published` branch).

Point a manual (non-Docker) SO-CRATES install at a locally-built AI summaries index so Suricata, Sigma, and YARA expansions show plain-English rule explanations.

```
$ AI_SUMMARIES_DIR=/opt/so-crates/summaries python3 socrates.py
```

— Names the env var, source repo/branch, and gives a runnable command. v3.2.0

---

03 **Security Onion Playbooks integration** NEW 88

`PLAYBOOKS_DIR` environment variable lets manual installs point at a locally-built Security Onion Playbooks index for Suricata and Sigma alert investigation guidance. Expanding a Suricata or Sigma alert now shows a Playbook section with plain-English investigation guidance sourced from Security Onion's Playbooks repository, baked into the Docker/Podman image.

Point a manual install at a locally-built Playbooks index so Suricata and Sigma alert expansions show investigation guidance.

```
$ PLAYBOOKS_DIR=/opt/so-crates/playbooks python3 socrates.py
```

— Names the env var and source, plus a runnable command. v3.2.0

---

04 **Whole-analysis notes via API** NEW 86

New `POST /api/analysis-notes` endpoint stores freeform analyst notes (e.g. 'suspected GuLoader, C2 at x.top') as `notes.txt` per analysis, supporting multi-line text and empty submission to clear. The notes icon in the analysis header and Previous Analyses list rows is muted when no notes exist and accent-colored once notes are present.

— Names the endpoint and storage file, with visual state cues. v3.1.0

---

05 **Full keyboard navigation across the app** IMPROVED 85

Keyboard navigation now covers the entire app: arrow keys move between stat-card tabs and data-table rows, Enter activates highlights (opens samples, expands/collapses rows), and Escape closes modals/menus one layer at a time before leaving an analysis. In Aggregation Tables specifically, Left/Right jumps between tables, Down walks rows and crosses into the next visual row of tables or the Data Table, and Enter activates Prev/Next pagination without losing focus. The Themes modal gained its own arrow-key grid navigation with live-preview on every move, jumping relative to the currently active theme. Keyboard reach was also extended to Sankey Diagram and Aggregation Tables

section headers (expand/collapse with Enter), aggregation table values, filter bar chips, and expanded-row detail panel elements (Add Note, ASCII Transcript, Hexdump, Download PCAP, Expand All/Collapse All, individual packets).

— Enumerates every key and UI surface but no single entry point shown. v4.1.0 v4.0.0

06 **Command palette for navigation and shortcuts** NEW 85

A command palette is triggered by typing any letter or digit outside a text field, supporting mid-word substring matching and ranked results for themes, stat-card tabs, and named shortcuts including `help`, `about`, `themes`, `rules`, `settings`, `notes`, `delete`, `re-analyze`, `search`, `clear`, `sankey`, `aggregation`, `advanced features`, `documentation`, `security onion`, `github repo`, `pcap samples`, `log samples`, `binary samples`, `upload`, `import`, `previous analyses`, `copy md5 hash to clipboard`, and `rename analysis`.

Quickly switch to a specific theme or jump to a feature without leaving the keyboard.

📍 Type `mp3` (outside any text field) to open the command palette pre-filled with `mp3`, then press Enter to switch to the MP3 Player theme. Type `re-analyze` and press Enter to re-run the current analysis.

— Full shortcut list plus a runnable trigger example. v4.0.0

07 **Alert acknowledgment workflow** NEW 85

`Acknowledge this alert` and `Acknowledge all instances of this alert` options in the pivot menu on Network Alert and Sigma Alert rows immediately remove acknowledged rows from all views (Network Alerts, Sigma Alerts, All Events, Sankey diagram, and counts). Acknowledged alerts appear in a new `Acknowledged Alerts` stat-card tab with per-type sub-sections and `Un-acknowledge this alert` support.

Silence a noisy Suricata signature firing hundreds of times so it no longer clutters any view during the current analysis.

📍 In the analysis view, right-click (or open the pivot menu) on any Network Alert or Sigma Alert row › select `Acknowledge all instances of this alert`. All matching rows are removed from Network Alerts, All Events, the Sankey diagram, and all counts immediately. To review or undo, open the `Acknowledged Alerts` stat-card tab and select `Un-acknowledge this alert`.

— Exact menu options and views affected, with a worked example. v4.0.0

08 **Pivot menu filters and threat-intel lookups** NEW 85

A new pivot menu on any table cell value offers Include, Exclude, Only, and Hunt filter actions, plus Copy to Clipboard and one-click lookups against Google, VirusTotal, Shodan, AbuseIPDB, urlscan.io, and CyberChef. It also supports user-defined custom

lookup sites — added, edited, or removed in Settings — using a `{value}` URL template, persisted per-browser with strict http/https-only URL validation.

Add a custom threat-intel lookup site so any pivot menu can open a value directly in your internal enrichment portal.

> 📍 In Settings, under Custom Lookup Sites, click Add and enter a name and URL using the `{value}` template — e.g. `https://intel.corp/search?q={value}` — then click Save. The entry is validated for http/https only and persisted per-browser.

— Names every lookup target and the exact template syntax, with steps. v3.2.0

---

09 **DNS tunneling and DGA heuristics tab** NEW 78

A new DNS Heuristics tab aggregates every DNS query by registrable domain and scores each 0–100 across five signals: high-entropy subdomain prefix (tunneling shape), high-entropy/low-vowel-ratio registrable domain (DGA shape), 15+ distinct subdomains under the same parent (fan-out), unusually long query name or label, and TXT/NULL record types. Known CDN suffixes are allowlisted before scoring to reduce noise.

— Names exact scoring signals and thresholds, but no example given. v4.1.0

---

10 **Inline analysis renaming** NEW 78

New `POST /api/rename-analysis` endpoint lets analysts rename an analysis display name inline; the original filename is preserved in `.meta`'s `original` field.

— Names the endpoint and metadata field but no example call. v3.1.0

---

11 **Parallel multi-file ZIP analysis** NEW 75

ZIP uploads containing multiple supported files now analyze every file independently in parallel (each pcap, log, or binary gets its own analysis) instead of silently dropping all but the first; byte-identical duplicates within the same ZIP are analyzed only once.

Analyze every pcap in a multi-file incident ZIP (e.g. from malware-traffic-analysis.net) in one upload instead of manually extracting and uploading each file.

> 📍 On the main screen, upload a `.zip` file containing multiple pcaps. SO-CRATES analyzes each supported file independently in parallel; a toast notification links to Previous Analyses where each result appears separately.

— Clear before/after behavior with a runnable upload example. v4.0.0

---

12 **Control relocation and theme-cycling key changes** BREAKING 75

The `t` key no longer cycles themes; theme-cycling moved to `<` / `>` keys, and theme switching is now handled through the command palette or Themes modal. Re-analyze and Delete controls moved off the Previous Analyses list onto the analysis page header, and Delete All moved into a new Danger Zone section in Settings. The Daylight theme was removed; users previously on Daylight are switched to White.

— Names exact keys and new locations for relocated controls. v4.0.0

13 **Community ID flow correlation** NEW 73

SO-CRATES now force-enables Suricata's `community_id` field on every analysis (off by default in Suricata) so flow and alert records can correlate against Zeek and other community-id-aware tools without manual configuration. A new Correlate entry in the pivot menu searches all logs across a capture sharing the same `community_id` flow — network protocol events and alerts alike — when clicking any field on a row that carries a community ID.

— Names the field and menu action but no worked example. v4.1.0

14 **New themes and ambient background updates** NEW 73

Adds a new MP3 Player fun theme (cheat code `mp3`) with brushed-metal chrome grays, LCD-green readout, and a bouncing spectrum-analyzer background. The Sguil theme moves from Fun Themes to Light Themes (retaining cheat code `sguil`). Ambient theme backgrounds were updated: Breadbin Blue and CGA gain demoscene-style plasma fields, with CGA's additionally quantized through a Bayer dither to the 4-color CGA palette, and Amber CRT now prints boot-log-style lines at randomized intervals. A new Themes interface also includes optional OhMyDebn theme sync.

— Names every theme and cheat code but no single command shown. v4.0.0 v3.1.0

15 **JA3/JA3S/JA4 TLS fingerprinting** IMPROVED 68

JA3, JA3S, and JA4 TLS client/server fingerprinting is now force-enabled on every analysis, whereas previously it was silently absent from `tls` events unless an active rule's signature keyword happened to require it. All three now appear as their own rows in a TLS row's detail panel when present.

— Clear before/after and named fields, only UI navigation to view. v4.1.0

16 **Per-row evidence annotations** NEW 65

A new note icon on Suricata alerts, DNS/HTTP/TLS/flow events, Sigma alerts, file/YARA matches, and imported log events lets analysts attach short annotations to individual evidence rows, separate from the whole-analysis Notes field.

— Names every row type covered but no example of use. v3.2.0

17 **Analysis date range field in list API** IMPROVED 65

`GET /api/analyses` now includes a `date_range` field (`{"min": ..., "max": ...}`, both `null` while still processing) per analysis, used for hover tooltips to distinguish same-named analyses.

— Names the exact field shape but no worked example. v3.1.0

---

18 **Automatic YARA/Sigma rule refresh** IMPROVED 65

YARA and Sigma cached rule files now refresh automatically if older than 24 hours and the network is reachable, falling back to the stale copy on failure. A single shared reachability probe replaces per-engine timeouts, capping startup delay at ~5s instead of ~15s.

— Explains the mechanism and numbers but needs no user action. v3.1.0

THINNER COVERAGE BELOW

19 **Opt-in protocol-decode alert tab** NEW 55

New `show_protocol_decode_alerts` setting in the Rules modal makes protocol-decode alert noise explicitly opt-in, with a dedicated Decoder Alerts tab shown when enabled.

— Names the setting but no example of using it. v3.2.0

---

20 **Reanalyze safeguards and quick access** IMPROVED 50

The reanalyze confirmation dialog now shows a bold warning and turns the Re-analyze button red when the analysis has unsaved row-level notes that would be destroyed. A new reanalyze icon in the analysis header re-runs the pipeline without leaving the page.

— Describes the warning behavior but no exact trigger flow. v3.2.0

---

21 **MD5 hash copy to clipboard** NEW 45

Clicking the MD5 hash in the analysis header copies it to the clipboard, with a toast confirming success or a clear error when `navigator.clipboard` is unavailable.

— Simple, fully described one-click action. v3.1.0

└──▷ ALSO FROM THESE RELEASES

.
.
.
.

└──▷ BREAKING ON UPGRADE

! The `t` key no longer cycles themes; theme-cycling moved to `<` / `>` keys, and theme switching is now handled through the command palette or Themes modal.

! The Daylight theme is removed; users previously on Daylight are switched to White.

! Re-analyze and Delete are no longer accessible from the Previous Analyses list on the welcome screen; they are now located on the analysis page header.

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Vulnerability Management

Rapid7 InsightVM

Feedback ⓘ 1 RELEASE · 2026-08-30 DOCS ↗

BLOG ↗

Rapid7 InsightVM is a vulnerability management platform that discovers, prioritizes, and remediates security risks across IT assets.

> InsightVM 8.57.0 adds compliance policy content for the latest DISA STIG benchmark covering Amazon Linux 2023.

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

01 DISA STIG Amazon Linux 2023 v1r4 policy content NEW

43

InsightVM 8.57.0 adds policy content for DISA STIG Amazon Linux 2023, Version 1 Release 4, enabling compliance assessments against the latest federal benchmark for Amazon Linux 2023 environments.

— Names exact benchmark and version but no scan/setup steps given. 2026-08-30-11cae43d

WAS THIS USEFUL? 👍 👎

Quarry VRC

Feedback

3 RELEASES · 2026-08-07 → 2026-08-19

NOTES ↗

Designed for managing vulnerability discovery at scale with agentic AI and integrates with HackerOne.

> Quarry VRC's launch (v1.3.3) shipped full HackerOne program/report sync, a Tracker and lead workflow, advisory feeds, a payload library, and a Bearer-token API for agentic access; v1.4.0 added Caido/Burp evidence capture and GraphQL-based HackerOne collaboration management; v1.5.0 layered on an incremental HackerOne poller, card/list views, and new dashboard stats.

└──▷ **WHAT SHIPPED · 19 FEATURES** most completely described first ? what's the number?

01 **HackerOne sync and incremental polling** NEW 91

Syncs HackerOne programs, scopes, reports, states, bounties, payout splits, and triage threads from the HackerOne API, and lets a finished report be filed directly to a program without copy-pasting into the web form. An incremental poller (`core/h1_watch.py`) detail-fetches only reports whose HackerOne list-endpoint change signals moved, recording state and bounty transitions as events to keep Tracker badges, the report-update feed, and bounty alerts current between full syncs; poll interval is tunable via `QUARRY_POLL_MINUTES` (default 15 minutes, set to `0` to disable the built-in timer and drive polls from an external scheduler).

Disable the built-in poller timer and drive HackerOne report polling from your own external scheduler (e.g. a cron job).

```
$ QUARRY_POLL_MINUTES=0
```

Reduce poll frequency to every 30 minutes to lower HackerOne API request volume in a low-traffic deployment.

```
$ QUARRY_POLL_MINUTES=30
```

— Names env var, defaults, and poller module. v1.5.0 v1.3.3

02 **Evidence capture from Caido and Burp** NEW 88

Adds `CAIDO_URL` and `BURP_URL` environment variables to point capture backends at Caido and Burp proxy instances (use `http://host.docker.internal:<port>` inside a container) for request/response and full-screen OS screenshot capture. New server routes and a CLI, including an `--attach` flag on the report-intent flow, record an

evidence timeline, a scope-filtered proxy feed, and support drafting and attaching files to reports.

— Names both env vars, CLI flag, and container usage. v1.4.0

03 **Private-data leak scanning in CI** NEW 81

Adds `scripts/check-no-private-data.sh` and CI workflow `.github/workflows/no-private-data.yml` to gate every commit, refusing home paths, LAN IPs, real report IDs, private handles, and credentials from reaching the repository.

Run the leak scanner locally before pushing to ensure no operator-private data (home paths, LAN IPs, report IDs, credentials) is committed.

```
$ bash scripts/check-no-private-data.sh
```

— Names exact script and workflow paths, runnable locally. v1.3.3

04 **Leads-by-class stats and Dashboard tile** NEW 73

Adds a `leads_by_class` breakdown to the `/api/stats` endpoint, powering a new Leads by class tile on the Dashboard.

Check the current leads-by-class breakdown from the stats API to populate dashboards or feed downstream tooling.

```
$ curl -s https://<quarry-host>/api/stats | jq '.leads_by_class'
```

— Names endpoint field and includes a runnable curl example. v1.5.0

05 **Tracker report table and lead workflow** IMPROVED 70

A Tracker shows every report with state, bounty, CWE, impact, and payout split; a lead workflow tracks states open, confirmed, ready, submitted, awarded, parked, and killed; and in-scope assets are mapped to local workspaces. The Tracker PRIV column renders a compact one-letter badge (N, L, or H), with High displayed in red and the full word retained in the hover title.

— Names workflow states and badge scheme, no direct command. v1.4.0 v1.3.3

06 **Configurable minimum password length** NEW 70

Adds `QUARRY_MIN_PASSWORD_LENGTH` environment variable (default 12) to enforce a configurable minimum password length for admin bootstrap and subsequent password changes.

Set a stronger minimum password length before bootstrapping the admin account in a production deployment.

```
$ QUARRY_MIN_PASSWORD_LENGTH=20
docker compose up -d
```

— Names exact env var, default, and example command. v1.3.3

07 **HackerOne collaboration management via GraphQL** NEW

68

New Integrations-tab card and stdlib GraphQL client for HackerOne let you list, accept, or reject program invitations; accept report-collaborator invitations; invite collaborators and set bounty splits. The browser session cookie is stored write-only and masked in the UI.

Adopt the vendor-neutral report and lead standards shipped with Quarry for consistent reporting across a team.

> 📍 In the Quarry VRC UI, go to the Integrations tab, then review and configure your HackerOne session cookie in the new HackerOne card; reference the standards in the `standards/` folder for report shape and lead lifecycle guidance.

— Names GraphQL client and invite/split actions, UI-only steps. v1.4.0

08 **Program discovery, visibility, and hacktivity tracking** NEW

62

An add-program picker searches every program a credential can see on HackerOne — including private and invited programs — and onboards one with its policy and scopes immediately populated. Programs are tracked with a Visibility column showing public / private / clear sourced from HackerOne, plus a screenshot-conceal toggle that blurs private program identities in demo screenshots. A program hacktivity tile on the Dashboard watches whichever program's public activity feed the operator selects.

— UI features described but no exact navigation given. v1.3.3

09 **Card and list views for Leads, Tracker, Advisories** NEW

60

Adds a card and list view across Leads, Tracker, and Advisories with a persisted toggle, equal-height cards with bottom-flush metadata, and PRIV plus C/I/A impact badges consistent with table mode.

— Names exact areas and badge scheme, no shortcut given. v1.5.0

THINNER COVERAGE BELOW

10 **Configurable advisory RSS/Atom feeds** NEW 59

Adds configurable RSS/Atom advisory feeds (CISA and VulDB by default, user-replaceable) parsed into Vendor / Product / Type columns and cross-referenced against your reports.

— Names default feeds and parsed columns, no config key given. v1.3.3

11 **Search and sort controls across Leads, Tracker, Programs, Targets, Payloads, Regression**

NEW 57

Adds a Search toggle and compact Sort control to Leads, Tracker, Programs, Targets, Payloads, and Regression, and applies the shared status-chip legend to Regression buckets.

— Names all six areas affected, no exact UI steps. v1.5.0

12 **Removed anticipated-award tracking and manual report form** 57

BREAKING

The anticipated (hand-recorded, unconfirmed-award) feature is removed from the Tracker, the report detail, and the Dashboard. The manual New report form is replaced with a How to submit link to the API-submit guide.

— Names removed surfaces but no migration steps given. v1.5.0

13 **Baseline security hardening** NEW 50

Ships standard hardening: IP allow-list checked before auth, TLS on first boot, PBKDF2-HMAC auth, write-only secrets, and a strict `default-src 'none'` CSP.

— Lists mechanisms but no config toggles to act on. v1.3.3

14 **Unified profile menu** IMPROVED 42

Adds a profile menu — a single account icon dropdown carrying the signed-in user, theme choice, and log out — replacing three separate top-bar chips.

— Describes UI change, no navigation path given. v1.5.0

15 **Vendor-neutral report and lead standards** NEW 40

New `standards/` folder ships vendor-neutral report and lead standards any Quarry hunter can adopt for a consistent report shape and lead lifecycle.

— Names the folder but not its contents in detail. v1.4.0

16 **Searchable payload library** NEW 38

Includes a searchable payload library cloned from PayloadsAllTheThings, one row per documented block.

— States source and structure, thin on usage. v1.3.3

17 **Bearer-token API for agent access** NEW 37

Provides a Bearer-token API so external scripts and agents can query the console without a browser session.

— No endpoint paths or token issuance steps given. v1.3.3

18 **Working retest-window control in Settings** IMPROVED 37

Adds a working retest-window control to Settings, replacing the previously unavailable cadence card.

— Names location but not the control's options. v1.5.0

19 **Files tab name filter and sorting** NEW 28

Adds a name filter and sortable columns to the Files tab.

— Bare description, no column names given. v1.5.0

└──▷ **BREAKING ON UPGRADE**

! The anticipated (hand-recorded, unconfirmed-award) feature is removed from the Tracker, the report detail, and the Dashboard.

! The manual New report form is replaced with a How to submit link to the API-submit guide.

WAS THIS USEFUL?  

GOVERN

◆ AI/LLM Security

ai-safe2-framework

Feedback ⓘ 1 RELEASE · 2026-08-29

NOTES ↗

The Universal Governance, Risk, Compliance (GRC) Operating System with Integrated Security for Agentic AI, Non-Human Identities, and Swarm Governance. AI SAFE² + AI Sovereignty Maturity Model (AISM), NEXUS-A2A Protocol, FORGE-Act, Marshal Plan for AI [Dual License: MIT + CC-BY-SA]

> AI SAFE² v3.1 adds machine-readable manifest and control datasets for automated consumers, six new MCP controls that bring the CP.5.MCP profile to 19 controls, a formal persistence vocabulary and enforcement-plane model, and re-anchors five existing MCP controls to framework-owned governance state with a twelve-month protocol migration window.

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

01 **Machine-readable manifest and entry points** NEW 80

Adds `ai-safe2.manifest.json` at the repository root as a deterministic machine entry point exposing framework version, component versions, normative paths, control counts, enforcement planes, persistence vocabulary, conformance boundaries, and machine-readable datasets. Also adds `AGENTS.md` as the canonical first-class entry point for automated consumers, `skills/mcp/data/mcp-profile-v3.1.json` as a machine-readable profile of the 19-control CP.5.MCP security profile, and `skills/mcp/data/ai-safe2-controls-v3.0.json` as the machine-readable 161-control core dataset.

— Names exact file paths but gives no consumption workflow v3.1

02 **Six new MCP controls (MCP-14 through MCP-19)** NEW 80

Adds MCP-14 (Extension Capability Negotiation), MCP-15 (Header and Body Assertion Integrity), MCP-16 (State Handle Binding and Lifecycle), MCP-17 (MRTR Round-Trip Integrity and Replay Resistance), MCP-18 (Catalog Cache Integrity and Provenance Revalidation), and MCP-19 (Authorization Chain Integrity, intended-resource/audience binding, and SSRF boundaries), bringing the CP.5.MCP profile to 19 controls. MCP-19 carries an explicit conformance boundary requiring deployments to evidence intended-resource, audience, or equivalent binding before protected dispatch — opaque bearer-token possession alone does not satisfy the control.

— Names each control and its conformance requirement, no runnable step v3.1

03 **Re-anchored MCP controls to framework-owned state** BREAKING 80

Re-anchors five existing MCP controls — MCP-4, MCP-7, MCP-8, MCP-11, MCP-13 — to framework-owned governance state (verified principals, capability grants, provenance baselines, delegation chains, governed state handles) instead of protocol session state, with primary binding to MCP `2026-07-28` and legacy compatibility with MCP `2025-11-25` for a twelve-month migration window.

— Names controls, versions, and migration window precisely v3.1

04 **Protocol-independent persistence vocabulary** NEW 60

Formalizes four canonical persistence values — `request`, `handle_scoped`, `durable`, and `swarm_shared` — replacing protocol-owned session language as the governance boundary.

— Names the four values but not where they're applied v3.1

05 **Three enforcement planes formalized** NEW 60

Formalizes three explicit enforcement planes — north-south (agent to model provider), east-west (agent to agent), and agent-to-tool (agent to MCP server or tool) — with the requirement that a control result on one plane does not establish coverage on another.

— Clear model and rule, but no config surface to act on v3.1

06 **Challenge Lab scoped by enforcement plane** NEW 60

Scopes the Challenge Lab and Challenge 001 by enforcement plane, adding v3.1 MCP cases covering header/body desynchronization, catalog/schema drift, replay, audience/resource confusion, endpoint impersonation, SSRF, and legacy state-handle misuse.

— Lists case types but no direct instructions to run them v3.1

THINNER COVERAGE BELOW

07 **Scanner rule registry expanded to 64 rules** IMPROVED 55

Expands the scanner rule registry from 52 pre-existing rules to 64 total by adding 12 new grouped CP.5.MCP v3.1 rules.

— Gives counts but not the rule names themselves v3.1

08 **Agent Discovery and Manifest Integrity CI gate** NEW 55

Adds a CI gate that verifies manifest claims against the actual repository, failing the build on incorrect claims and broken paths.

— Describes gate behavior but not the check name or invocation v3.1

09 **Standardized navigation shell across docs** IMPROVED

35

Standardizes repository navigation and context shell across all 18 direct example README surfaces and all 24 numbered research notes under a common v3.1 shell.

— Documentation formatting change with no operational surface v3.1

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · August 30, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue