THE CYBER TOOLCHAIN

NO. 100

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED OCTOBER 10, 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 62 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 18 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.

PROTECT

Work the vulnerability queue by what attackers are using, not by
ss

vim ? help

Findings now carry CISA Known Exploited Vulnerabilities status and a computed remediation deadline, so the KEV cross-reference that teams were doing in a spreadsheet or a BI job happens at the finding. The patch list sorts by evidence of real-world exploitation and by the date you owe the fix.

Datadog Cloud Security

DETECT

Answer "what domain did this beacon resolve from" without three pivots

A new API endpoint and CLI subcommand link DNS, connection, protocol and alert records together, and a capture-time flag writes DNS answers onto connection records as they are seen. Attribution of an IP back to the hostname that produced it stops being a manual correlation across logs and becomes a field a detection rule can match on.

Netcap

PROTECT

Put a policy gate between an AI agent and the tools it can call

Arcjet's Agent Guards enforces rules on agent tool calls at runtime, with dry-run rollout and native hooks so coding agents are covered without an SDK; Corridor's `analyzePlan` MCP tool steers an agent before it generates code, backed by a maintained Repository Threat Model. Both move the control from reviewing agent output after the fact to constraining what it is allowed to do.

Arcjet · Corridor

PROTECT

Catch a poisoned JavaScript dependency before npm install runs it

Chainguard Libraries verifies JavaScript lockfiles through `chainctl`, which matters because install scripts execute on resolution — checking after install is checking after the compromise. Noir added 60+ framework and language targets across Salesforce, .NET, JVM, PHP and Python, widening the codebases it can read to find undocumented API routes.

Chainguard · noir

OFFENSIVE SECURITY

◆ Reconnaissance & OSINT

OpenOSINT Feedback ⓘ v2.32.0 NOTES ↗

AI-powered OSINT agent with interactive REPL, MCP server, and CLI. 20 tools.

Adds keyless geolocated news ingestion from the GDELT GKG feed with no API key required.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v2.32.0
https://github.com/OpenOSINT/OpenOSINT.git
# already have the repo? check out this version:
$ git checkout v2.32.0
```

NEW INTEGRATION GDELT GKG feed integration

WAS THIS USEFUL? 👍 👎

◆ Hacking Hardware

JustCallMeKoko LLC ESP32 Marauder v8 Feedback ⓘ

sold out · Oct 9, 2026 STORE ↗

The official handheld ESP32-C5 board for the ESP32 Marauder firmware, with a touchscreen, dual-band Wi-Fi 6, Bluetooth 5 and GPS for Wi-Fi and BLE auditing and wardriving.

Marauder v8 (marauder-v8) sold out at justcallmekokollc.com on 9 Oct 2026.

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

Mend.io Mend Platform

Feedback ⓘ changelog · Oct 10, 2026

CHANGELOG ↗ RANK

Traditional application security misses AI risk. Standalone AI security tools miss your code.

> Mend Renovate shipped three small engineering improvements this window: smarter env/config merging, a simplified Docker build, and stronger internal type safety.

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

01 **Strong typing for Containerbase tools in util/exec** IMPROVED

35

Adds a strong type for Containerbase's known tools in `util/exec`, improving type safety for tool invocations.

— Names code location but is an internal, non-user-facing change product docs

02 **Containerbase Sidecar removed from Docker build** IMPROVED

30

Removes the Containerbase Sidecar image from the Docker build process, simplifying the container build pipeline.

— Explains what changed but no actionable detail for users product docs

NEW INTEGRATION Invicti Platform DAST integration

NEW INTEGRATION Port.io platform integration for SCA findings

changelog · Oct 10, 2026 CHANGELOG ↗ LATEST STABLE

Mend Platform adds zero-day alerts, a centralized Activity Log with API export, account-level global workflows, IDE-based finding suppression via Agentic Integrations, and a unified SCA remediation experience.

Adds dedicated zero-day alerts for immediate awareness when your organization is vulnerable to emerging threats, toggleable per organization via My Profile → Email Notifications.

Adds a new Send Email action in Automation Workflows to notify of new findings independent of scans, with configurable delivery frequencies.

Enhances Automation Workflows email notifications to allow workflow creators to select specific users or groups as recipients for scan summary emails.

> Introduces a suppression tool in Agentic Integrations enabling single and bulk suppression or unsuppression of findings across SAST and SCA engines directly within IDE or AI agent workflows, with UI updates reflected within seconds.
>
> Introduces unified vulnerability remediation across the Mend Platform, adding a `Top Fix` column in the Findings table and standardizing fix logic and recommendations in the Remediation tab.
>
> +8 more

WAS THIS USEFUL?  

Semgrep

Feedback ⓘ snapshot-20261010 NOTES ↗

Get started with Semgrep to help you catch, flag, and fix real vulnerabilities before they ship.

Tag API endpoints now require dedicated tag permissions; read-only tokens gain SBOM/Supply Chain API access; Guardian gains SLSA Level 3 verification and auto-update with opt-out controls.

Deployment tag API endpoints now require tag-specific API permissions: use a token with tag read permission for `GET` `/list` /find operations and tag write permission for update/delete operations.

Read-only API tokens can now call the v1 Supply Chain dependency and SBOM export endpoints, which previously required an admin-only scope.

Running AI analysis or opening an Autofix pull request now requires triage permission; read-only users receive an explanatory error.

Adds `SEMGREP_GUARDIAN_AUTO_UPDATE=0` environment variable and `auto_update: false` key in `guardian.yaml` to opt out of Semgrep Guardian's new automatic self-update behavior.

Semgrep Guardian 2.5.4 and later checks for updates and downloads new binaries immediately on release rather than waiting up to a week for the coding agent to re-index the repository.

+1 more

NEW INTEGRATION Cursor Origin SCM integration

NEW INTEGRATION AWS CodeArtifact registry support (private beta)

NEW SUPPORTED PLATFORM Network Broker scms field for private SCM instances

└─▷ **BREAKING ON UPGRADE**

! Deployment tag API endpoints now require tag-specific permissions; a token that previously managed projects is no longer sufficient — obtain a token with tag read permission for GET/list/find and tag write permission for update/delete.

WAS THIS USEFUL? 👍 👎

GitHub Feedback ⓘ

GitHub Copilot weekly releases — October 5 (2026-10-09) BLOG ↗ RANK

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

> GitHub shipped weekly Copilot updates (local-model discovery in the CLI, GA local sandboxing, multi-account app support, Claude Haiku 5.5), new organization-level billing and access controls for Copilot code review, and CodeQL 2.27.2 with new C/C++, Rust, Go and JavaScript/TypeScript analysis plus several breaking changes to the Go CFG, macOS build support, and deprecated IfStmt APIs.

└──▷ **WHAT SHIPPED · 17 FEATURES** most completely described first ? what's the number?

01 Go control-flow graph migrated to shared CFG library BREAKING

85

The Go control-flow graph now uses the shared CFG library: `BasicBlocks::Cfg` is removed, and CFG nodes, edges, locations, textual representations, and basic-block boundaries have changed, requiring queries built on the previous representation to be updated. The migration also adds `ControlFlow::EntryNode`, `ControlFlow::ExitNode`, and `SwitchStmt.getExpr` to the Go CFG.

— Describes mechanism and before/after but no migration command

CodeQL 2.27.2 improves C++, Go, Rust, a…

02 Org billing and access controls for Copilot code review NEW

85

Organizations gain a Choose how members with a Copilot license are billed setting under org `Copilot -> Policies`, with Member (default, bills the member's own entitlement) and Organization (bills the repository-owning org via AI Credits paid usage, with an optional budget) options, plus an Only allow Copilot code review to be triggered by authorized users toggle (org and repo level) to block review requests made with external or personal Copilot licenses.

Switch Copilot code review billing to the organization cost center so member quotas are never consumed or exhausted.

> 📍 In your organization settings, go to Copilot -> Policies, locate 'Choose how members with a Copilot license are billed', and select Organization. Ensure AI Credits paid usage is enabled for the org, then optionally set a budget.

Restrict Copilot code review requests to users holding an org- or enterprise-issued license, blocking personal or external licenses org-wide.

> 📍 In your organization settings, go to Copilot -> Policies and enable 'Only allow Copilot code review to be triggered by authorized users'. Once set at the org level, repository admins cannot override it.

— Exact setting names, options, and navigation steps given

Copilot code review: New organization b…

---

03 **`--dil-constants` flag for `codeql query compile`** NEW

80

`codeql query compile` gains a `--dil-constants` flag, used together with `--dump-dil`, to include optimized constant tuple sets in the emitted DIL output for query debugging.

Inspect optimized constant tuple sets during query development to understand how the compiler resolves constants.

```
$ codeql query compile --dump-dil --dil-constants my-query.ql
```

— Exact flag and runnable command provided CodeQL 2.27.2 improves C++, Go, Rust, a…

---

04 **Trusted-owner exclusion in `actions/unpinned-tag` query**

IMPROVED

75

The `actions/unpinned-tag` query's trusted-owner set now supports `!-prefixed` entries (e.g. `!github`) to exclude an owner from the trusted list, allowing first-party unpinned tags such as GitHub-owned Actions to be reported.

Report unpinned tags from first-party GitHub-owned Actions (owner `github`) by removing them from the default trusted set.

```text
!github
```

— Named query and exact config syntax with example

CodeQL 2.27.2 improves C++, Go, Rust, a…

---

05 **Model discovery via `/model` in Copilot CLI** NEW

70

Copilot CLI gains a `/model` command that lists and lets you switch between models from a running local Ollama instance as well as already configured and cloud models, enabling mid-session model switching for lower-latency or offline inference.

Switch to a locally-running model mid-workflow without leaving the CLI — useful when you want lower-latency or offline inference via Ollama.

```
$ /model
```

— Names exact command and gives a runnable example

GitHub Copilot weekly releases — Octobe…

06 **macOS 27 build-mode support restricted** BREAKING 70

CodeQL autobuild and manual build modes are no longer supported for compiled languages on macOS 27 (any Xcode version) or on macOS 26 with Xcode 27 selected; supported environments are capped at macOS 26 with Xcode 26.

— Gives explicit supported-environment migration guidance

CodeQL 2.27.2 improves C++, Go, Rust, a…

07 **IfStmt and LoopStmt API deprecations** DEPRECATED 70

`IfStmt.getCond` is deprecated in favor of `IfStmt.getCondition`; the return types of `IfStmt.getThen` and `LoopStmt.getBody` change to `Stmt`; and several IR instruction classes are consolidated.

— Names exact deprecated and replacement APIs CodeQL 2.27.2 improves C++, Go, Rust, a…

08 **New C/C++ sink models and regex parsing** NEW 65

C/C++ analysis gains SQL-injection sink models for the Comdb2 C API, flow summaries for Bloomberg BDE codecs and byte-stream deserializers, and parsing of regular expressions that use the ECMAScript grammar in `std::regex`.

— Names all affected APIs though no direct action

CodeQL 2.27.2 improves C++, Go, Rust, a…

09 **Session management additions to VS Code Agents window** NEW 60

The VS Code Agents window adds side-by-side agent session viewing with a grid layout to compare results or follow multiple tasks concurrently, and an Open worktree cleanup action in VS Code chat that surfaces disk usage of inactive session worktrees and lets you remove selected ones.

— Names two concrete UI features in the same surface

GitHub Copilot weekly releases — Octobe…

10 **Rust analysis flow summaries and extractor classes** NEW 60

Rust analysis adds flow summaries for `native-tls`, `async-native-tls`, and `tokio-native-tls`, and extractor support for `AnyAttr` and `DocComment` classes.

— Names crates and classes but no usage path CodeQL 2.27.2 improves C++, Go, Rust, a…

THINNER COVERAGE BELOW

11 **Local sandboxing reaches general availability** IMPROVED 55

Local sandboxing is now generally available across Copilot CLI, the Copilot app, and VS Code sessions using Agent Host, limiting agents' access to files, networks, and credentials at no extra cost.

— States scope and benefit but no config surface to act on

GitHub Copilot weekly releases — Octobe…

12 **Clickjacking recognition improved in missing-x-frame-options query**

IMPROVED 55

The `cs/web/missing-x-frame-options` query now recognizes ASP.NET Core response headers and Content Security Policy `frame-ancestors` directives as valid clickjacking protections, reducing false positives.

— Names query and mechanism but no reproduction steps

CodeQL 2.27.2 improves C++, Go, Rust, a…

13 **Razor tag-helper values no longer flagged as XSS sinks**

55

BREAKING

The `cs/web/xss` query no longer treats Razor tag-helper attribute values written with `WriteLiteral` as XSS sinks, which may remove previously reported findings.

— Clear before/after but no remediation command CodeQL 2.27.2 improves C++, Go, Rust, a…

14 **Multi-account support in Copilot app** NEW 50

The Copilot app now supports using separate GitHub accounts for a Copilot license and for repository access — for example pairing an enterprise-provided Copilot license with a personal repository account — via separate account settings in the app.

— UI path described with illustrative screenshot GitHub Copilot weekly releases — Octobe…

15 **Go websocket import path modeling extended** NEW 50

Go analysis now models the `github.com/coder/websocket` import path alongside the existing `nhooyr.io/websocket` path.

— Names exact import paths, thin on mechanism CodeQL 2.27.2 improves C++, Go, Rust, a…

16 **Workflow SDK directive recognition in JS/TS analysis** NEW

50

JavaScript/TypeScript analysis now recognizes the Workflow SDK's `'use workflow'` and `'use step'` directives.

— Named directives, minimal further detail CodeQL 2.27.2 improves C++, Go, Rust, a…

17 **Claude Haiku 5.5 added to Copilot** NEW

35

Claude Haiku 5.5 is now available as a selectable model to Copilot Pro, Pro+, Max, Business, and Enterprise users.

— Names plans but no usage mechanism GitHub Copilot weekly releases — Octobe…

└──▷ ALSO FROM THESE RELEASES

▶ Watch video

└──▷ BREAKING ON UPGRADE

! CodeQL autobuild and manual build modes are not supported for compiled languages on macOS 27 (any Xcode version) or on macOS 26 with Xcode 27 selected; use at most macOS 26 and Xcode 26.

! The Go CFG now uses the shared CFG library: `BasicBlocks::Cfg` is removed; CFG nodes, edges, locations, textual representations, and basic-block boundaries have changed — queries relying on the previous representation must be updated.

! `IfStmt.getCond` is deprecated in favor of `IfStmt.getCondition`; the return types of `IfStmt.getThen` and `LoopStmt.getBody` change to `Stmt`; several IR instruction classes are consolidated.

! The `cs/web/xss` query no longer treats Razor tag-helper attribute values written with `WriteLiteral` as XSS sinks, which may remove previously reported findings.

WAS THIS USEFUL? 👍 👎

Veracode

Feedback ⓘ Integration updates (2026-10-09) BLOG ↗

RANK

Veracode is a cloud-based application security platform that performs static, dynamic, and software composition analysis to identify vulnerabilities in code.

> Veracode's integration updates add new veracode.yml pipeline controls for pre-packaging scripts, IaC policy checks and branch-scoped scans, change default Git metadata collection behavior, and introduce Veracode Fix for SCA in GitHub alongside new VS Code extension configuration screens — while also flagging a required Azure DevOps Extension v4.0.0 migration and the end of support for Jira Server/Data Center 9.x.

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

01 New veracode.yml pipeline scan configuration options NEW

85

veracode.yml pipeline configuration gained `predependency_command` to run a pre-packaging setup script before Veracode scans a project in a GitLab or Azure DevOps pipeline, `policy` to apply an IaC policy check (e.g. `policy: 'Veracode Recommended Medium'`) as part of a GitHub, GitLab, or Azure DevOps workflow scan, and `analysis_branch` to restrict scheduled Azure DevOps scans to a specific analysis branch rather than the default branch.

Run a pre-packaging setup script before Veracode scans your project in a GitLab or Azure DevOps pipeline.

yaml

```yaml
# veracode.yml
predependency_command: pip install -r requirements.txt
```

Apply an IaC policy check as part of a GitHub, GitLab, or Azure DevOps workflow scan.

yaml

```yaml
# veracode.yml
policy: 'Veracode Recommended Medium'
```

Restrict scheduled Azure DevOps scans to a specific analysis branch rather than the default branch.

```yaml
# veracode.yml
analysis_branch: main-security
```

— Three named config keys with runnable YAML snippets for each.

Integration updates (2026-10-09)

---

02 **Azure DevOps Extension v4.0.0 migration from v3** BREAKING

75

Veracode Azure DevOps Extension v4.0.0 requires manually migrating existing pipelines from v3 to v4 for both Azure DevOps Server and Azure DevOps (Cloud); the deprecated Veracode Flaw Importer v3 task is replaced by the `VeracodeFlawImporter` v4 task.

— Names old and new task versions, lacks step-by-step migration guide.

Integration updates (2026-10-09)

---

03 **End of support for Jira Server/Data Center 9.x integration**

DEPRECATED

70

Veracode will end support for the Veracode Integration for Jira on Jira Server and Jira Data Center 9.x on November 30, 2026; customers must upgrade to Jira 10 or later to continue using a supported version.

— Exact deadline and upgrade path given, no migration mechanics.

Integration updates (2026-10-09)

THINNER COVERAGE BELOW

---

04 **`-repourl` flag now required for Git metadata updates**

55

BREAKING

Java API wrapper v26.10.20.1 changes Git metadata collection so that the repository URL in the Veracode application profile is updated only when `-repourl` is explicitly specified, rather than automatically.

— Flag and version named but no usage example given. Integration updates (2026-10-09)

---

05 **VS Code extension install, settings, and proxy setup** NEW

30

Documentation screenshots show the Veracode VS Code extension installation flow, a settings tab, policy menu settings, and a proxy setting screen, consistent with the summary's mention of new platform-based install and schedule workflows.

— Only screenshot alt-text available; no prose description of behavior.

Integration updates (2026-10-09)

06 **Veracode Fix for SCA in GitHub** NEW 15

Veracode Fix for SCA is now available as part of GitHub integrations, per the release summary; no further detail on scope or mechanism was provided in this window.

— Mentioned only in summary with no supporting detail. Integration updates (2026-10-09)

└──▷ **BREAKING ON UPGRADE**

! Veracode Azure DevOps Extension v4.0.0 requires manually migrating existing pipelines from v3 to v4 for both Azure DevOps Server and Azure DevOps (Cloud); the deprecated Veracode Flaw Importer v3 task is replaced by `VeracodeFlawImporter` v4.

! Veracode will end support for the Veracode Integration for Jira on Jira Server and Jira Data Center 9.x on November 30, 2026; upgrade to Jira 10 or later to continue using a supported version.

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

humble

Feedback ⓘ 1.67 NOTES ↗ RANK

A humble and fast security-oriented HTTP headers analyzer.

> humble 1.67 expands its detection database with new insecure header checks and a fingerprint header, improves XML export output, and refines the verbose check alongside several unspecified feature additions.

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

01 **Expanded insecure header and fingerprint detection** NEW

32

Adds 7 new insecure header checks, expanding detection of deprecated or insecure header values, and adds 1 new fingerprint header to the fingerprint detection database.

– Counts given but no specific header names or mechanism. 1.67

02 **Verbose check refinement** IMPROVED

28

Improves the `-v` verbose check.

– Names the flag but gives no behavioural detail. 1.67

03 **Improved XML export output** IMPROVED

18

Significantly improves the XML export output.

– No detail on what changed in the export. 1.67

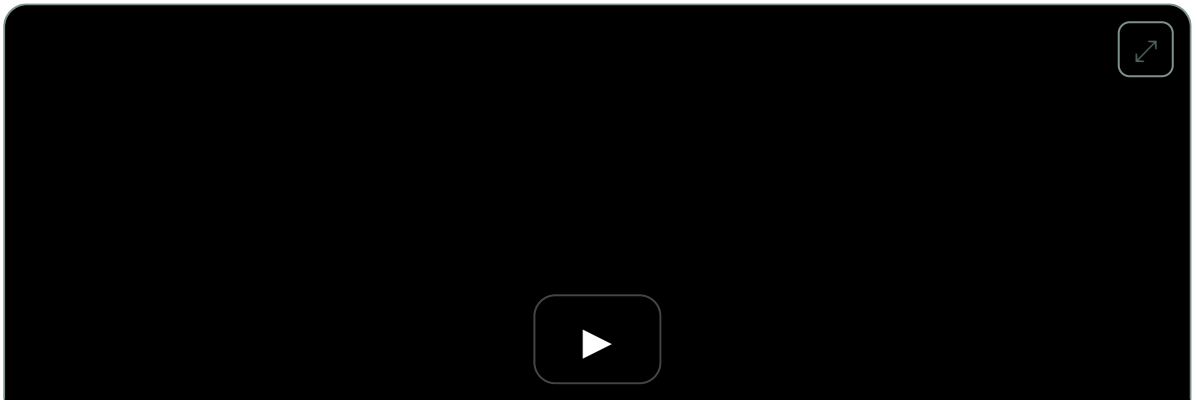
04 **Unspecified feature additions across two commits** NEW

18

Adds 4 new features (details in extended commit message for commit `127f815`) and 3 new features (details in extended commit message for commit `da29ca2`).

– Commit hashes given but actual feature content undisclosed. 1.67

└──▷ **ALSO FROM THESE RELEASES**





WAS THIS USEFUL? 👍 👎

◆ WAF, Bot & API Protection

Levo

Feedback ⓘ SaaS Platform Services -- 1.2.135.7 NOTES ↗ RANK

Continuous API Security Assurance a observe, detect, and protect your APIs.

> Levo's SaaS platform now surfaces license status directly in the UI and enforces test budgets on web application scans, while changing license fields in its Workspace and Organization APIs in a breaking way.

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

01 In-product license status and expiry warnings NEW

45

The product UI now surfaces license status, including expiry warnings, a grace period, and end-of-access enforcement, so users can see licensing state without leaving the product.

– Describes UI behavior but no exact navigation path given

SaaS Platform Services -- 1.2.135.7

02 Test budget enforcement for web application scans IMPROVED

45

Web application scans now enforce a test budget, ensuring scans finish within the allotted budget while still recording every distinct finding.

– Explains mechanism but no config key or limit value given

SaaS Platform Services -- 1.2.135.7

03 Breaking change to license fields in Workspace/Organization APIs

45

BREAKING

License fields in the Workspace and Organization APIs have changed; any integration that reads those fields must be updated before upgrading.

– Names affected APIs and required action but no field names

SaaS Platform Services -- 1.2.135.7

└──▷ **BREAKING ON UPGRADE**

! License fields in the Workspace and Organization APIs have changed — any integration that reads those fields must be updated before upgrading.

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

mac_apt

Feedback ⓘ v.1.36.2 NOTES ↗ RANK

macOS (& ios) Artifact Parsing Tool

> mac_apt v1.36.2 adds five new artifact plugins covering calculator history, Authkit daemon identity data, WiFi configuration, XProtect, and Safari tags.

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

01 New plugins for calculator, AKD, WiFi, XProtect, Safari tags

NEW 75

Adds a `CALCULATOR` plugin to read calculator history from macOS artifacts; an `AKD` plugin to read device and email alias info from Authkit daemon (`com.apple.akd`) databases; parsing of `wifiagent.plist` for wifi artifact collection; support for a new `XPdb` location in XProtect artifact parsing; and reading of Safari tags via the `SAFARI` plugin.

Extract calculator history from a disk image to identify recently computed values during an investigation.

```
$ python mac_apt.py -i <image.dmg> -o <output_dir> CALCULATOR
```

Pull Authkit daemon identity data (device info and email aliases) from a macOS image to map Apple ID associations.

```
$ python mac_apt.py -i <image.dmg> -o <output_dir> AKD
```

— Names all five plugins/paths; only two have runnable commands shown. v.1.36.2

WAS THIS USEFUL? 👍 👎

◆ Network Analysis & Monitoring

Netcap

Feedback ⓘ v0.13.0 NOTES ↗ CODE ↗ RANK

A framework for secure and scalable network traffic analysis - https://netcap.io

> Netcap v0.13.0 adds cross-protocol evidence linking that joins DNS, connection, protocol and alert records through a new API endpoint and CLI subcommand, plus a capture-time flag that snapshots DNS answers onto connection records for detection rules.

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

01 Cross-protocol evidence linking across DNS, connections and alerts

NEW 96

Adds the `--evidence-links` flag (env `NC_EVIDENCE_LINKS`) to enable/disable cross-protocol evidence linking in the web UI and via the new `GET /api/evidence/related` endpoint, retrievable also through the `net investigate related` subcommand, which links DNS, connections, protocol records and alerts into a timeline. Bounds are configurable via `--evidence-links-window` (env `NC_EVIDENCE_LINKS_WINDOW`, default 1h) limiting the time between a DNS answer and a connection, `--evidence-links-max-records` (env `NC_EVIDENCE_LINKS_MAX_RECORDS`, default 1,000,000) capping indexed records per output directory, and `--evidence-links-max-links` (env `NC_EVIDENCE_LINKS_MAX_LINKS`, default 500) limiting related records returned per query; exceeding these limits is reported as truncation. Links are bound to audit-file content hashes and enforce capture interface/VLAN scope, withholding ambiguous joins instead of guessing, and a Settings → Features UI panel toggles evidence linking and network detections independently at runtime.

Limit cross-protocol evidence linking to a 30-minute window and cap results at 100 links per query to reduce memory use on large captures.

```
$ ./net capture -read traffic.pcap --service --evidence-links --evidence-links-window 30m --evidence-links-max-links 100
```

— Full flags, env vars, defaults, endpoint and limits all named v0.13.0

02 Capture-time DNS resolution context for detection rules NEW

70

Adds the `--dns-resolution-context` flag (env `NC_DNS_RESOLUTION_CONTEXT`) to snapshot matched UDP DNS answers onto Connection records, letting capture-time

detection rules match on the DNS name that resolved a connection's destination.

Capture from a PCAP file with DNS resolution context enabled so that detection rules can match on the DNS name that resolved a connection's destination.

```
$ ./net capture -read traffic.pcap --service --dns-resolution-context
```

— Names flag and env var but mechanism detail is brief v0.13.0

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Runtime Security

Alibaba Cloud OpenSandbox

Feedback ⓘ release-1.1.1

NOTES ↗ RANK

Secure, Fast, and Extensible Sandbox runtime for AI agents.

> OpenSandbox shipped identity-bound filesystem execution, chained upstream proxy egress with corporate CA trust, Kubernetes multi-tenant isolation and pause/resume, plus new CLI subcommands for template and snapshot management, across two releases.

└──▷ **WHAT SHIPPED · 12 FEATURES** most completely described first ? what's the number?

01 Upstream proxy egress via config and env vars NEW

95

Adds `[egress.upstream_proxy]` config section (URL + optional authorization) that injects a chained upstream CONNECT proxy for both Docker and Kubernetes backends, with `ca_cert_path` (Docker) and `ca_secret_name` (Kubernetes) to trust private-CA `https://` proxies without replacing the system trust store. Also adds `OPENSANDBOX_EGRESS_UPSTREAM_PROXY` and `OPENSANDBOX_EGRESS_UPSTREAM_PROXY_AUTH` environment variables to route transparent-proxy egress through an upstream CONNECT proxy with SNI/Host-consistent authority and fail-closed startup validation.

Route all sandbox egress through a corporate CONNECT proxy signed by an internal CA, without replacing the sidecar system trust store.

ini

```ini
[egress.upstream_proxy]
url = "https://proxy.corp.example.com:3128"

# Docker deployments
ca_cert_path = "/etc/pki/corp-ca.pem"

# Kubernetes deployments
# ca_secret_name = "corp-ca-secret"
```

— Config keys, env vars and runnable config example all present release-1.1.1 release-1.1.1-rc.1

02 Identity-bound filesystem operations NEW

90

Adds identity-bound filesystem operations via `/v1/filesystem/{uid}/{gid}` execd routes, backed by a per-request worker running with explicit Linux UID/GID credentials,

exposed as `files_with_identity` (Python) and `filesWithIdentity` (JavaScript, Kotlin, Go, C#) across all five SDKs.

— Endpoint, worker mechanism and all SDK method names given `release-1.1.1`

03 **Host-address binding for bridge-mode ports** NEW 90

Adds `[docker] publish_host` config key to bind bridge-mode sandbox ports to a specific host address (default `0.0.0.0`), preventing the tokenless execd port from appearing on public interfaces when set to `127.0.0.1` or the Docker bridge gateway.

Lock sandbox port exposure to localhost so the tokenless execd port never reaches public interfaces on a Docker host.

ini

```
[docker]
publish_host = "127.0.0.1"
```

Lock down the tokenless execd port so it is never reachable on public interfaces in a Docker deployment.

ini

```
[docker]
publish_host = "127.0.0.1"
```

— Exact key, default, and example config provided `release-1.1.1` `release-1.1.1-rc.1`

04 **CLI subcommands for template and snapshot management** NEW 90

Adds `osb template create|get|list|delete` and `osb snapshot ...` CLI subcommands, plus `--template` and `--snapshot-id` flags on `sandbox create`, for template and snapshot management. Also adds a kubectl-style `-f` / `--file` flag to `sandbox create` and `template create` for full wire-format request files with strict unknown-field rejection.

Create a sandbox from a full wire-format YAML file in CI, and start it from a named template with a snapshot pinned.

```
$ osb sandbox create -f sandbox-spec.yaml --template my-base-template --snapshot-id snap-abc123
```

— Exact subcommands, flags and a runnable CLI example given `release-1.1.1-rc.1`

05 **Multi-overlay mounts for isolated sessions** NEW 85

Exposes `CreateIsolatedSessionRequest.overlays` (`{path, mode, persist}`) across the API and all five SDKs, enabling multiple independent overlay mounts per isolated session with separate host-tracked or ephemeral tmpfs uppers; `workspace` is retained as sugar and `SessionState` echoes the canonical list.

– Full field schema and behaviour given, no runnable example `release-1.1.1`

---

06 **Pause/resume for agent-sandbox provider** NEW 85

Implements pause/resume for the agent-sandbox provider by bridging to `spec.operatingMode` (`Running` / `Suspended`) on `agents.x-k8s.io/v1beta1`, with state derivation (`Paused` / `Pausing` / `Resuming` / `Terminated`) and a 409 response on invalid transitions.

– API field, states and error code all named `release-1.1.1`

---

07 **Template env baked into golden image** NEW 80

Accepts `env` on template create, baking it into the fast-sandbox golden image at `/etc/sandbox-init.env` (inheriting the source image's OCI `Config.Env`), supported across all five SDKs.

– File path, inheritance behaviour and SDK scope named `release-1.1.1`

---

08 **Typed HTTP statuses for proxied backend failures** IMPROVED 75

Maps proxied backend failures to typed HTTP statuses: read/write timeouts return `504 BACKEND_TIMEOUT`, mid-response resets and protocol errors return `502 BACKEND_RESPONSE_FAILED`, and connect failures return `502 BACKEND_CONNECTION_FAILED`.

– Exact status codes and triggers listed, no usage example `release-1.1.1`

---

09 **Persistent env var injection via commands.setEnv** NEW 70

Adds `commands.setEnv` across all five sandbox SDKs (Python async/sync, JavaScript, Kotlin/Java, Go, C#) for persistent runtime environment variable injection, appending `KEY=VALUE` to the sandbox env file at runtime.

– Mechanism and SDK coverage named, no code sample `release-1.1.1`

10 **Tenant isolation in shared Kubernetes namespace** NEW

70

Isolates tenants sharing one Kubernetes namespace via a new `opensandbox.io/tenant` stamp label — list/get/delete/pause/resume/proxy operations hide other tenants' labeled sandboxes as 404s, while unlabeled legacy sandboxes remain visible until expiry.

— Label mechanism and 404 behaviour given, no CLI example `release-1.1.1`

11 **Access-renew opt-out header** NEW

65

Adds `OpenSandbox-Access-Renew: skip` request header to opt individual requests out of access renew intents, for health probes and heartbeat-style traffic.

— Exact header and value given, no runnable example `release-1.1.1-rc.1`

THINNER COVERAGE BELOW

12 **Insecure TLS skip for Kubernetes ServiceAccount CA mismatches**

NEW

55

Adds `kubernetes.insecure_skip_tls_verify` config key for ServiceAccount CA mismatches in Kubernetes multi-tenant deployments.

— Single config key named, no mechanism detail beyond that `release-1.1.1`

WAS THIS USEFUL?  

DETECTION & RESPONSE

◆ SIEM

Databricks

Feedback ⓘ

Code execution in Genie One (Public Preview) (2026-10-09) BLOG ↗ RANK

Databricks is a unified analytics platform for data engineering, data science, and machine learning built on Apache Spark.

> Databricks added sandboxed code execution to Genie One, a new faster evaluator model for LLM-as-a-judge policies, and request-tag enforcement in Unity Gateway service policies.

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

01 **OpenJev evaluator for LLM-as-a-judge policies** NEW

55

Databricks adds OpenJev (Qwen3.5 4B) as a selectable evaluator model service in custom LLM-as-a-judge service policies. It classifies content without generating output tokens, making it faster than a chat evaluator. Currently in Beta.

– Names model and mechanism but no setup steps given

Use OpenJev as the evaluator for LLM-as…

02 **Code execution in Genie One** NEW

45

Genie One can now run code in a secure, isolated sandbox for advanced analyses beyond SQL, using the user's existing Unity Catalog permissions and data access controls. Currently in Public Preview.

– Explains mechanism and access model but no config/flag named

Code execution in Genie One (Public Pre…

03 **Request tags in Unity Gateway service policies** NEW

45

Unity Gateway service policies can now evaluate caller-supplied request tags, allowing a policy to require a tag be present before a model request or MCP tool call proceeds. Currently in Beta.

– Describes enforcement behavior without a concrete config example

Use request tags in Unity Gateway servi…

WAS THIS USEFUL? 👍 👎

Sumo Logic

Feedback ⓘ

Dynamic Timeslice Drilldown on Dashboard Log Panels (Dashboards) (2026-10-09)

BLOG ↗ RANK

Sumo Logic is a cloud-based platform for log management, monitoring, and security analytics of applications and infrastructure.

> Sumo Logic dashboards gained dynamic timeslice drilldown, letting users zoom into log panel spikes with automatic query resolution recalculation.

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

01 Dynamic timeslice drilldown on dashboard log panels NEW

55

Click and drag to zoom into a time range on a dashboard log panel, and Sumo Logic automatically recalculates the query's timeslice and re-fetches the panel at finer resolution, enabling spike and anomaly investigation without editing the underlying query.

Drill into a traffic spike on a log panel without touching the underlying query.

> 📍 In a Sumo Logic Dashboard, open a log panel displaying a timeslice-based chart. Click and drag over the spike region to zoom in — Sumo Logic automatically recalculates the timeslice and re-fetches the panel at the finer resolution.

— Explains mechanism and UI path, but no config/API surface named.

Dynamic Timeslice Drilldown on Dashboar…

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

Trend Vision One

Feedback ⓘ

Assess AI application readiness with OWASP AISVS scoring in AI Scanner (2026-10-09)

BLOG ↗ RANK

Trend Vision One is Trend Micro's cloud-based XDR platform providing unified security visibility and threat detection across endpoints, networks, and cloud environments.

> Trend Vision One's AI Scanner adds time-series analytics with longer result retention and per-scan timestamps, plus mTLS client-certificate authentication for custom AI endpoints.

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

01 mTLS client-certificate auth for custom AI endpoints NEW

86

AI Scanner adds a `target.custom.tls` config block with `cert_env`, `key_env`, and `ca_env` fields to supply client certificate and private key material (PEM, via environment variables) for mTLS-authenticated custom AI endpoints. This mTLS authentication can be used alone or combined with existing API key or cookie authentication.

Scan a custom AI endpoint protected by mTLS with a private CA, injecting the certificate material via environment variables so secrets never appear in config files.

yaml

```yaml
target:
  custom:
    tls:
      cert_env: AI_CLIENT_CERT
      key_env: AI_CLIENT_KEY
      ca_env: AI_CA_CERT
```

— Exact config keys and runnable YAML example provided

Scan mTLS-protected custom AI endpoints…

02 AI Scanner time-series charts and extended retention IMPROVED

67

The AI Scanner dashboard gains Results over time and Attack success rate over time charts showing distinct successful attacks broken down by severity for a selected target, with a per-day/per-scan toggle to switch between aggregated and individual-run views. Successful attacks are deduplicated when multiple scans share a data point, scan results

retention is extended from 60 days to 180 days, and every scan result now carries a timestamp visible in the results table and finding details.

Track whether a target is improving or regressing over weeks without manually comparing individual scan reports.

> 📍 In the Trend Vision One console, go to AI Security -> AI Application Security -> AI Scanner, select your target, and open the `Results over time` or `Attack success rate over time` chart. Use the per-day / per-scan toggle to switch between aggregated and per-run views.

— Names charts, retention change, and UI path; no API given

`Chart AI Scanner results over time with…`

NEW COMPLIANCE FRAMEWORK OWASP AISVS 1.0 scoring

NEW DETECTION AISVS attack preset covering prompt injection, output safety, memory, orchestration, and adversarial robustness

> `Assess AI application readiness with OWASP AISVS scoring in AI Scanner (2026-10-09)`
>
> **BLOG ↗** **STABLE**
>
> AI Scanner adds OWASP AISVS 1.0 per-level scoring (Level 1/2/3) with pass rates visible in the dashboard, executive summary, and exported reports.
>
> Scores AI application scans against OWASP AISVS 1.0 at three ascending levels — Level 1 (baseline), Level 2 (sensitive data), and Level 3 (high-risk/critical) — each reporting a pass rate and a verdict of PASS, PASS (partially assessed), NOT ASSESSED, or FAIL.
>
> Surfaces AISVS scores in the dashboard, executive summary, and exported reports, with drill-down from each level to the individual requirement, a link to the standard, and a direct jump to the failed attack in the results table.
>
> Adds AISVS scoring access under AI Security → AI Application Security.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

SailPoint

Feedback ⓘ

Enhancement: ServiceNow Service Catalog v5.4 — Event-driven Approvals and Access Request

BLOG ↗ RANK

SailPoint is an identity governance and access management platform that automates user provisioning, access reviews, and compliance across enterprise systems.

> SailPoint's ServiceNow integration moved from polling to real-time ISC event triggers, the collaboration portal gained flexible SSO identity matching, and Access Risk Management added deep SAP Fiori app visibility across risk rules, reviews and reports, alongside smaller ARM usability updates.

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

01 **Event-driven ISC-ServiceNow sync (v5.4)** BREAKING 95

ServiceNow Service Catalog v5.4 adds five ISC event trigger subscriptions via `https://{instance_name}.service-now.com/api/x_sap_intidn/isc_event_processor` to push real-time approval and access-request state changes from Identity Security Cloud to ServiceNow, replacing timer-based polling. An ISC Backup Utility scheduled job reconciles missed events during connectivity or event-delivery failures, and an ISC Event Processing Table Cleaner job purges old event records with a default 7-day retention period configurable via the Data Management Policy. Configuring the event triggers is mandatory from v5.4 — polling no longer works — so customers must create a ServiceNow integration user (roles `rest_service`, `x_sap_initidn.user`, `itil`; identity type Machine, web services access only), subscribe to and validate all five triggers, confirm the Identity Security Cloud Links table includes v5.4 endpoints, and activate the Data Management Policy and table cleaner rule.

Configure the ISC Event Processing Table Cleaner retention window to match your company data policy.

> 📍 In ServiceNow, navigate to the Data Management Policy for the ISC Event Processings table, activate the table cleaner rule, and set the retention period (default: 7 days) to your required value.

— Names endpoint, jobs, retention default and full migration checklist.

Enhancement: ServiceNow Service Catalog…

02 **SAP Fiori app tracking across ARM risk and reviews** BREAKING

85

Enabling `Include Fiori Metadata` on the SAP connection in the ARM agent (on by default for new connections) activates Fiori app tracking via the `ZARM_FIORI_META` dictionary and `ZARM_UTIL_DATA` Launchpad plugin. Rulebook risk definitions now support Fiori intents with the `[FAPP]` prefix and OData services with the `[SVC]` prefix alongside transaction codes — existing unprefixed Fiori rulebook entries must be updated before the next rulebook import or they will stop matching. A new Fiori report lists which roles and catalogs grant which Fiori apps and OData services, with or without usage, filterable by Fiori Application ID. The emergency access activity grid now shows Fiori intents and OData services with a readable description (e.g. `(F2223) Reset Cleared Items`), a sensitivity flag, and a Standard or Elevated marker; User to Role periodic access reviews show Fiori intents and execution counts; and role-level utilization reports include Fiori app usage so reviewers can see what a user would lose before a role is removed. Admins can also choose to keep collecting raw OData service calls from the SAP Security Audit Log independently of app-level Fiori usage.

During an emergency access review, inspect exactly which Fiori apps an elevated user opened — with plain-language names, sensitivity flags, and Standard vs. Elevated markers.

> 📍 In ARM, open an emergency access review for the target session and check the activity grid — Fiori rows appear alongside transactions, each labeled with its Application ID and description (e.g. `(F2223) Reset Cleared Items`) and an Elevated marker if the access came only from the elevated session.

— Names dictionary, plugin, prefixes and every surfaced report/review, but no exact command path.

New Capability: SailPoint ARM brings Fi…

---

03 **Login Lookup Mode for collaboration portal SSO** NEW

80

Adds a `Login Lookup Mode` setting on the collaboration portal SSO tab, letting administrators choose between `NameID` (default) and `Assertion attribute` matching to resolve SSO identity-mapping failures when an IdP transforms or hashes the user identifier. Assertion-attribute matching (for example, email) works for both pre-provisioned (non-JIT) and JIT user flows, and is configurable through the admin UI and API.

When your IdP transforms or hashes the NameID, switch the collaboration portal SSO matching mode to assertion attribute so pre-provisioned collaborators can authenticate.

> 📍 In the admin UI, go to the collaboration portal SSO tab, locate the `Login Lookup Mode` setting, and select `Assertion attribute`. Then coordinate with your identity team to map the correct SAML attribute (for example, email) in the IdP.

— Names exact setting, both modes and UI path with worked example.

Enhancement: Collaboration Portal SSO -…

THINNER COVERAGE BELOW

04 **Quoted phrase search in ISC Access Object Search** NEW

50

Wrapping multi-word terms in double quotes in the Name, Description, or Additional Search fields of the ISC Access Object Search widget now matches a contiguous phrase; unquoted searches behave as in v5.3.

— Names the widget and fields but no step-by-step example given.

Enhancement: ServiceNow Service Catalog…

05 **OOTB connector for ARM JML access via ISC** NEW 40

Adds a new out-of-the-box (OOTB) connector to manage Access Risk Management users' JML (Joiner-Mover-Leaver) access through ISC.

— Names the connector's purpose but no setup detail or mechanism.

New Capability: SailPoint ARM brings Fi…

06 **Admin-editable user email in ARM** NEW 30

ARM admins can now edit a user's email address directly in the product, without contacting support.

— Bare description of a small UI capability, no navigation path.

New Capability: SailPoint ARM brings Fi…

07 **Navigation overhaul for ARM reporting** IMPROVED 25

Delivers a side and top navigation overhaul for customers not on legacy reporting.

— Mentions a UI redesign with no scope or specifics.

New Capability: SailPoint ARM brings Fi…

NEW INTEGRATION Disconnected applications connector

└──▷ **BREAKING ON UPGRADE**

! Configuring ISC event triggers is mandatory from v5.4 — existing timer-based polling is replaced and will not function; customers must create a ServiceNow integration user (roles `rest_service`, `x_sap_initidn.user`, `itil`; identity type Machine, web services access only), subscribe to the five required event triggers, validate each subscription, verify the Identity Security Cloud Links table includes v5.4 endpoints, and activate the Data Management Policy and table cleaner rule before the integration will operate.

! Existing rulebook entries for Fiori that lack a prefix must be updated: Fiori intents now require the `[FAPP]` prefix and OData services require the `[SVC]` prefix before the next rulebook import, or they will not match correctly.

Enhancement: Disconnected applications connector - limited availability (2026-10-09)

BLOG ↗ STABLE

New disconnected applications connector governs API-less web apps via browser-extension UI recording for provisioning, deprovisioning, and aggregation in ISC.

Adds the SailPoint connectivity browser extension to record administrator UI workflows once and replay them for automated provisioning, deprovisioning, and aggregation against web apps that expose no API.

Introduces the disconnected applications connector as a new source type in Identity Security Cloud, bringing legacy web apps, custom internal tools, and API-less systems under centralized SailPoint governance.

Enables zero-code connectivity by letting administrators map recorded UI inputs to SailPoint identity attributes (such as name or email) without writing custom scripts.

Surfaces accounts and entitlements from disconnected applications in SailPoint's existing search, certifications, reporting, and reconciliation workflows alongside connected sources.

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

CISO Assistant

Feedback ⓘ v4.1.1 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.

Adds EBIOS RM on MCP, risk owner and asset capabilities on MCP server, third-party tiering, flexible forms, paginated external API workflows, and a visual framework aggregator.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v4.1.1 https://github.com/intuitem/ciso-assistant-community.git
# already have the repo? check out this version:
$ git checkout v4.1.1
```

Expands MCP server with `asset objectives/capabilities`, `entity relationship`, and `list_objects` types.

Adds risk owner capabilities to the MCP server.

Makes advanced EBIOS RM available on the MCP server.

Introduces tiering capabilities for third parties and a more flexible forms engine.

Expands CEL capabilities to frameworks, enabling cyfun 2025 framework to benefit from them.

+7 more

NEW COMPLIANCE FRAMEWORK ISO 27001 to HDS mapping

NEW COMPLIANCE FRAMEWORK PIPL and PI compliance frameworks for Chinese market

NEW COMPLIANCE FRAMEWORK OWASP SAMM v2.2 library

NEW COMPLIANCE FRAMEWORK IEC 62443 mapping with ANSSI recommendations

UPDATED INTEGRATION ServiceNow integration pagination past ACL-short pages

WAS THIS USEFUL? 👍 👎

◆ Integrated & IT Risk Management

LogicGate

Feedback ⓘ

How to Report on Provision 29 with Confidence: Insights from LogicGate & PwC (2026-10-09)

BLOG ↗ RANK

LogicGate Risk Cloud is the leading AI-powered GRC platform with 30+ applications for enterprise risk, third-party risk, cyber risk and compliance management.

> LogicGate launched a purpose-built Provision 29 compliance application built with PwC, unifying risk taxonomy, control testing, and board-ready reporting, alongside new PwC-led readiness workshops for the provision.

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

01 **Provision 29 compliance application** NEW 75

LogicGate added a Provision 29 application on the AI GRC Platform, built in partnership with PwC, giving teams a unified workspace for risk taxonomy, assurance plans, and board-ready control-effectiveness reporting. It can be deployed standalone or layered on top of existing Enterprise Risk Management and Internal Audit Management applications, letting teams import existing risks and controls and flag them as material without reworking data. A single board dashboard shows control effectiveness by domain (financial, operational, reporting, and compliance), open remediation, and testing coverage across all three lines of defense, and one-click declaration generation pulls the latest control results, automatically flags repeat exceptions, and documents every corrective action plan.

— Describes app, dashboard, and declaration flow but no exact UI path or API

How to Report on Provision 29 with Conf…

THINNER COVERAGE BELOW

02 **Provision 29 readiness workshops** NEW 40

LogicGate and PwC offer tailored 60-minute Provision 29 readiness workshops and community working sessions covering board reporting, scoping, and deficiency tracking.

— Names the offering but no sign-up or access details given

How to Report on Provision 29 with Conf…

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

NVIDIA OpenShell

Feedback ⓘ v0.1.3 NOTES ↗

OpenShell runs autonomous AI agents in policy-controlled sandboxes with isolated filesystem, network, and credential access.

v0.1.3 adds OCSF JSONL gateway audit events, bearer auth passthrough, OTLP traces from sandbox supervisors, Ctrl-D session detach, gateway capacity metrics with optional HPA, VM host-tool preflight checks, runtime image env overrides, and optional cluster-scoped RBAC in Helm.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v0.1.3 https://github.com/NVIDIA/OpenShell.git
# already have the repo? check out this version:
$ git checkout v0.1.3
```

Adds `feat(cli): detach sandbox sessions with Ctrl-D` — press Ctrl-D to detach from a running sandbox session without terminating it.

Adds `feat(server): write gateway OCSF events to JSONL` — the gateway now emits structured audit events in OCSF JSONL format.

Adds `feat(helm): configure gateway OCSF JSONL output` — Helm values expose controls for enabling and routing the gateway's OCSF JSONL audit stream.

Adds `feat(service): add bearer authorization passthrough` — the gateway service layer can forward bearer tokens from inbound requests to upstream endpoints.

Adds `feat(supervisor): export OTLP traces from sandbox supervisors` — sandbox supervisors now emit OpenTelemetry traces over OTLP for distributed tracing pipelines.

+10 more

NEW INTEGRATION Oracle Cloud Infrastructure Generative AI provider profile

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · October 10, 2026

Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue