THE CYBER TOOLCHAIN

NO. 087

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED SEPTEMBER 27, 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 23 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 4 tools

▾ // THE BRIEF HIDE

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

Three unrelated things stand out. GitGuardian now strips secrets out of model context on more coding assistants and agent CLIs, so a pasted doesn't leave the laptop. Plerion extended workload scanning

vim ? help

across Azure compute families with attack-path and exploit checks. Lookyloo surfaces console messages, WebAuthn and OPFS from a capture, and auto-tags .onion hosts.

PROTECT

Keep secrets out of what the AI coding assistant sends upstream

AI Hooks now withholds secrets from model context across more assistants and covers new agent CLIs, so a credential sitting in the open file or shell history isn't shipped to a third-party model as ambient context. The configurable ggshield API timeout is the quieter win: monorepo scans that previously died mid-run and got waved through now finish.

GitGuardian SaaS

PROTECT

Cover the Azure compute you were quietly skipping

Workload scanning now reaches nearly every Azure compute family, with attack path findings, exploit checks and registry access permissions behind it. Agentless coverage gaps are where unpatched VMs hide; closing the family list means the console inventory and the scanned inventory finally match, and a vulnerable host is ranked by whether it's actually reachable rather than by CVSS alone.

Plerion

DETECT

See what a page did, not just what it loaded

Captures now expose console messages, WebAuthn and OPFS entries, which is where obfuscated loaders and browser-side persistence leave traces that never appear in the HAR. Onion Lookup integration auto-tags .onion hosts during capture, with optional push to AIL, so an analyst stops hand-checking whether a hidden service is already known.

Lookyloo

GOVERN

Show an auditor the evidence without exporting the database

v4.0.7 adds a downloadable audit log, risk trajectory tracking and batch control management, plus an overhauled x-rays module with domain-level checks. Trajectory turns a static risk register into something you can show moving over a quarter, and batch edits remove the click-per-control slog that makes framework mappings go stale.

CISO Assistant

APPLICATION SECURITY

◆ Secrets Detection & Management

GitGuardian SaaS

Feedback ⓘ

AI Hooks keep leaked tool output away from the model (2026-09-25) BLOG ↗

RANK

GitGuardian SaaS is a cloud-based security platform that detects and prevents secrets leakage in git repositories and source code.

> GitGuardian SaaS made ggshield's API timeout configurable to stop large-repo scans from failing, and expanded AI Hooks to withhold secrets from model context on more coding assistants while extending coverage to new agent CLIs.

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

01 Configurable API timeout for ggshield scans IMPROVED

90

ggshield previously enforced a fixed 60-second API timeout that could cause large-repo scans to fail with read timeouts. A new `api_timeout` config key (set in `~/.gitguardian/.gitguardian.yaml`) and a `GITGUARDIAN_API_TIMEOUT` environment variable let users raise this limit, e.g. `GITGUARDIAN_API_TIMEOUT=120 ggshield secret scan repo .` or `api_timeout: 120` in the config file.

Prevent large-repo scans from failing with a read timeout by raising the API timeout above the old 60-second hard limit.

📍 `GITGUARDIAN_API_TIMEOUT=120` ggshield secret scan repo .

Set a persistent API timeout in the ggshield config file so every scan honours the higher limit without needing an environment variable.

```yaml
api_timeout: 120
```

Raise the API timeout when large scans are failing with read timeouts in CI or on slow networks.

```yaml
api_timeout: 120
```

Override the API timeout via environment variable in a CI pipeline where the config file is not available.

📍 `GITGUARDIAN_API_TIMEOUT=120` ggshield secret scan repo .

— Names config key, env var, file path, and runnable commands.

AI Hooks keep leaked tool output away f…

02 AI Hooks coverage extended to Kiro and Junie CLI NEW

80

AI Hooks and the AI agents/MCP inventory now cover Amazon Kiro (IDE and CLI) and Junie CLI, blocking secrets in commands and file reads. A new `ggshield machine setup` subcommand registers AI Hooks for Kiro and Junie CLI in one step.

Register AI Hooks for Kiro and Junie CLI on a developer workstation after upgrading to ggshield 1.55.0.

```
$ ggshield machine setup
```

— Names exact new subcommand and the covered integrations.

AI Hooks keep leaked tool output away f…

03 AI Hooks withhold leaked tool output from model IMPROVED

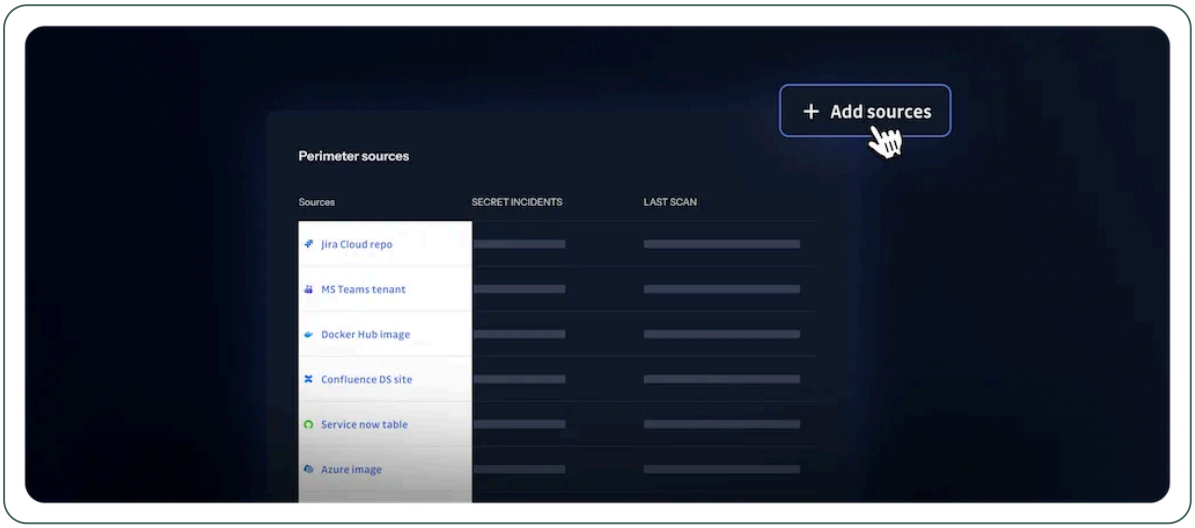
60

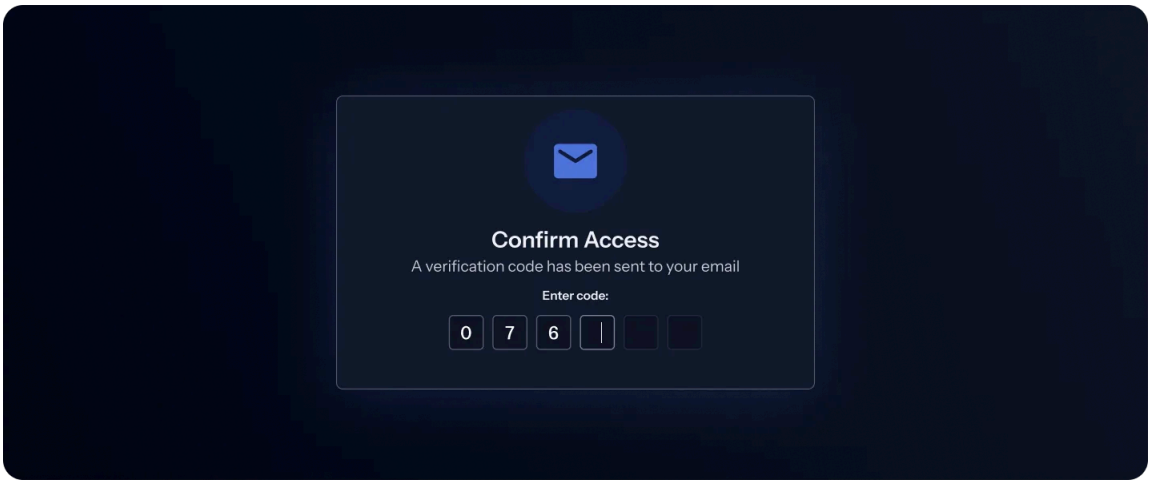
AI Hooks now withhold shell-command output containing secrets from the model context on Claude Code, Codex, and Mistral Vibe — the assistant receives only the ggshield message, keeping the secret out of the model session transcript.

— Explains mechanism and before/after but gives no setup step.

AI Hooks keep leaked tool output away f…

└──▷ ALSO FROM THESE RELEASES





AI Hooks keep leaked tool output away from the model (2026-09-25) BLOG ↗

LATEST STABLE

AI Hooks now withhold tool output from Claude Code, Codex, and Mistral Vibe, and extend coverage to Kiro and Junie CLI.

└──▷ **USE IT**

Raise the API timeout when large scans are failing with read timeouts in CI or on slow networks.

```yaml
api_timeout: 120
```

Register AI Hooks for Kiro and Junie CLI on a developer workstation after upgrading to ggshield 1.55.0.

```
$ ggshield machine setup
```

Override the API timeout via environment variable in a CI pipeline where the config file is not available.

📍 `GITGUARDIAN_API_TIMEOUT=120` ggshield secret scan repo .

Adds `api_timeout` config key and `GITGUARDIAN_API_TIMEOUT` environment variable to override the previously fixed 60-second API timeout.

Adds `ggshield machine setup` subcommand to register AI Hooks for Kiro and Junie CLI in one step.

AI Hooks now withhold shell-command output containing secrets from the model context on Claude Code, Codex, and Mistral Vibe — the assistant receives only the ggshield message, keeping the secret out of the model session transcript.

> Extends AI Hooks and the AI agents/MCP inventory to cover Amazon Kiro (IDE and CLI) and Junie CLI, blocking secrets in commands and file reads.

WAS THIS USEFUL?  

CLOUD & CONTAINER SECURITY

◆ CNAPP

Plerion

Feedback ⓘ

Azure workload scanning covers every workload family: NOTES ↗ RANK

Plerion is a cloud security platform that discovers and manages vulnerabilities and misconfigurations across infrastructure.

> Plerion expanded Azure workload scanning to cover nearly every Azure compute workload family, backed by new attack path findings, exploit checks, registry access permissions, and inventory coverage.

└──▷ **WHAT SHIPPED · 5 FEATURES** most completely described first ? what's the number?

01 Azure workload scanning expands to new workload types NEW

78

Vulnerability, sensitive data, and SBOM scanning now covers Azure App Service web apps, Virtual Machine Scale Sets, Container Apps, Container Instances, and Batch pools, in addition to previously covered virtual machines and functions. Service Fabric node types are covered through their underlying scale sets, and Uniform-orchestration scale sets are sampled by image, scanning one member per distinct image. Each workload type must be enabled individually under the subscription's workload scanning settings.

Enable scanning for newly supported workload types on an Azure subscription so Container Apps and Batch pools are included in vulnerability and SBOM assessments.

> 📍 In the Plerion console, go to the subscription's Workload Scanning Settings and toggle on App Service web apps, Container Apps, Container Instances, and Batch pools.

— Names workload types, scan types, sampling mechanism, and toggle path

Azure workload scanning covers every wo…

02 New exploit checks for container and Batch pool images NEW

60

Six new Azure checks flag exploitable and known-exploited vulnerabilities in container workload and Batch pool images: `PLERION-AZURE-452` (Container App exploitable), `PLERION-AZURE-453` (Container App known-exploited), `PLERION-AZURE-454` (Container Instance exploitable), `PLERION-AZURE-455` (Container Instance known-exploited), `PLERION-AZURE-459` (Batch pool image exploitable), and `PLERION-AZURE-460` (Batch pool image known-exploited).

— Names all six checks but no direct reader action

Azure workload scanning covers every wo…

THINNER COVERAGE BELOW

03 Attack path findings for exposed vulnerable workloads NEW

50

Plerion generates attack path findings for publicly exposed Azure workloads that have high or critical severity vulnerabilities, flagged via check `PLERION-AZURE-446`.

— Names the check but no reader action described Azure workload scanning covers every wo…

04 AcrPull permission for scanning appliance NEW

45

The Azure install script now grants `AcrPull` to the appliance identity so container images stored in Azure Container Registries can be pulled and scanned.

— Names the permission but action is automatic via install script

Azure workload scanning covers every wo…

05 Inventory coverage for OpenShift, Service Fabric, Batch NEW

25

Plerion's inventory now includes OpenShift, Service Fabric, and Batch resources.

— Brief statement with no mechanism or reader action

Azure workload scanning covers every wo…

Azure workload scanning covers every workload family: NOTES ↗ LATEST STABLE

Plerion Azure workload scanning expands to App Service, VM Scale Sets, Container Apps, Container Instances, and Batch pools

└──▷ **HOW TO FIND IT**

Enable scanning for newly supported workload types on an Azure subscription so Container Apps and Batch pools are included in vulnerability and SBOM assessments.

📍 In the Plerion console, go to the subscription's Workload Scanning Settings and toggle on App Service web apps, Container Apps, Container Instances, and Batch pools.

Extends vulnerability, sensitive data, and SBOM scanning to Azure App Service web apps, Virtual Machine Scale Sets, Container Apps, Container Instances, and Batch pools — in addition to the virtual machines and functions already covered.

Covers Service Fabric node types through their underlying scale sets.

Samples Uniform-orchestration scale sets by image, scanning one member per distinct image.

Generates attack path findings for publicly exposed workloads with high or critical vulnerabilities (`PLERION-AZURE-446`).

> Grants `AcrPull` to the appliance identity via the install script so container images in Azure Container Registries can be pulled for scanning.
>
> +3 more

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Threat Intelligence

Lookyloo

Feedback ⓘ v1.41.1 NOTES ↗ RANK

Lookyloo is a web interface that allows users to capture a website page and then display a tree of domains that call each other.

> Lookyloo's v1.41.1 release expands capture data exposure to include console messages, WebAuthn, and OPFS entries, adds a large-deployment kvrocks tuning sample, and integrates Onion Lookup for automatic .onion tagging with optional AIL push.

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

01 **Kvrocks config sample for large deployments** NEW 65

Adds a kvrocks config sample at `full_index/kvrocks.conf-big_instance` for tuning large deployments.

— Exact file path given but no tuning specifics v1.41.1

THINNER COVERAGE BELOW

02 **Onion Lookup integration for .onion tagging** NEW 50

Lookyloo integrates with Onion Lookup to automatically tag `.onion` captures and optionally push full captures to AIL.

— Names integration and behavior but no config detail v1.41.1

03 **Expanded browser data capture exposure** NEW 40

Lookyloo now gathers and renders browser console messages during captures, and exposes WebAuthn entries and Origin Private File System (OPFS) entries discovered during page captures.

— Names three data types exposed but no mechanism or UI path v1.41.1

v1.41.1 NOTES ↗ LATEST STABLE

Lookyloo v1.41.1 adds console message capture, WebAuthn/OPFS exposure, and onion-site tagging via Onion Lookup.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v1.41.1
https://github.com/Lookyloo/lookyloo.git
# already have the repo? check out this version:
$ git checkout v1.41.1
```

Adds a kvrocks config sample at `full_index/kvrocks.conf-big_instance` for tuning large deployments.

Gathers and renders browser console messages during captures.

Exposes WebAuthn entries discovered during page captures.

Exposes Origin Private File System (OPFS) entries discovered during page captures.

Integrates with Onion Lookup to automatically tag `.onion` captures and optionally push full captures to AIL.

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

CISO Assistant

Feedback ⓘ v4.0.7 NOTES ↗ RANK

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.

> CISO Assistant v4.0.7 adds in-app notifications, a downloadable audit log, risk trajectory tracking, an overhauled x-rays module with domain-level checks, and Mermaid diagram support in documentation, alongside batch control management and Helm chart flexibility.

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

01 Mermaid diagram support in documentation fields NEW

70

Adds Mermaid diagram support in markdown documentation fields — insert a fenced code block with the `mermaid` language tag to embed architecture or threat-model diagrams alongside control descriptions.

Embed a Mermaid architecture or threat-model diagram directly in a documentation field to keep visual context alongside control descriptions.

> 📍 In a markdown documentation field, insert a fenced code block with the `mermaid` language tag — e.g.: `mermaid graph LR A[Asset] --> B[Control] B --> C[Risk]`

— Runnable example with exact syntax provided v4.0.7

THINNER COVERAGE BELOW

02 Batch ETA date on applied controls NEW

55

Adds batch mode on applied controls to set an ETA date across multiple controls at once, via a batch actions menu that lets users select controls and choose Set ETA date.

Set an ETA date on multiple applied controls at once to keep remediation timelines visible across a programme.

> 📍 In Applied Controls, select the controls you want to update, open the batch actions menu, and choose Set ETA date.

— Exact UI steps given for a runnable action v4.0.7

03 Downloadable audit log (pro) NEW

50

Adds a downloadable audit log (pro tier) so teams can export a full activity trail for compliance evidence or incident investigation.

Download the full audit log to review who changed what and when — useful for compliance evidence or incident investigation.

> 📍 In the pro console, go to Audit Log and click the Download button to export the activity trail.

— Names exact UI path to download the log `v4.0.7`

---

04 **Helm chart: custom command/args, Qdrant image, managed OIDC keys**

NEW — 50

Adds custom command/args, Qdrant image, and managed OIDC key options to the Helm chart.

— Names three concrete Helm options, no key names or values `v4.0.7`

---

05 **X-rays module: domain-level checks and evidence flagging**

IMPROVED — 45

The x-rays page is reworked to add domain-level x-rays checks that surface compliance and control gaps at the domain scope, plus flagging of active controls that lack evidence.

— Names two concrete checks but no exact UI steps `v4.0.7`

---

06 **Applied controls on audit via data wizard and CLI** NEW — 35

Adds support for applied controls on audit via the data wizard and CLI.

— Names concrete surfaces (data wizard, CLI) but no usage detail `v4.0.7`

---

07 **Controls status column in findings binder** NEW — 30

Adds a controls status column to the findings binder view.

— Names exact view but no further mechanism `v4.0.7`

---

08 **In-app notifications center** NEW — 25

Adds an in-app notifications center for real-time alerts within the platform.

— Described only in prose, no config or UI path given `v4.0.7`

---

09 **Risk trajectory and projection view** NEW — 25

Adds a risk trajectory and projection view to track how risk posture changes over time.

— No mechanism or navigation detail given `v4.0.7`

10 **Real TTP techniques on EBIOS operational scenarios** NEW 25

Adds real TTP techniques exposed on EBIOS operational scenarios.

— Names the EBIOS feature but no mechanism detail v4.0.7

11 **Organisation-scoped custom feature flags** NEW 25

Allows users to redefine their own feature flags within the boundaries of their organisation.

— No config key or flag names given v4.0.7

12 **Workflow enablers and AI blocks** IMPROVED 20

Adds more workflow enablers — documents, tasks, and validations — and improved AI blocks.

— Generic list with no specifics on what changed v4.0.7

v4.0.7 NOTES ↗ LATEST STABLE

CISO Assistant v4.0.7 adds in-app notifications, audit log download, risk trajectory, domain-level x-rays, and Mermaid diagram support.

└──▷ GET THIS VERSION

```
$ git clone --branch v4.0.7 https://github.com/intuitem/ciso-assistant-community.git
# already have the repo? check out this version:
$ git checkout v4.0.7
```

└──▷ HOW TO FIND IT

Download the full audit log to review who changed what and when — useful for compliance evidence or incident investigation.

📍 In the pro console, go to Audit Log and click the Download button to export the activity trail.

Set an ETA date on multiple applied controls at once to keep remediation timelines visible across a programme.

📍 In Applied Controls, select the controls you want to update, open the batch actions menu, and choose Set ETA date.

Embed a Mermaid architecture or threat-model diagram directly in a documentation field to keep visual context alongside control descriptions.

📍 In a markdown documentation field, insert a fenced code block with the `mermaid` language tag — e.g.: `mermaid graph LR A[Asset] --> B[Control] B --> C[Risk]`

Adds in-app notifications center for real-time alerts within the platform.

Adds downloadable audit log (pro) so teams can export a full activity trail.

Adds risk trajectory and projection view to track how risk posture changes over time.

Adds domain-level x-rays checks to surface compliance and control gaps at the domain scope.

Adds x-rays flagging for active controls that lack evidence, with a reworked x-rays page.

+8 more

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · September 27, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue