THE CYBER TOOLCHAIN

NO. 027

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED JULY 27, 2026 · EVERY WEEKDAY

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

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // **CONTENTS** SHOW 20 tools

OFFENSIVE SECURITY

◆ AI-Powered Offensive Security

Strix ⓘ v1.4.0 NOTES ↗

Open-source AI penetration testing tool to find and fix your app's vulnerabilities.

Strix v1.4.0 adds self-update, ChatGPT inference, Linux ARM64, Bedrock prompt caching, and smarter context management for long scans.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.4.0 https://github.com/usestrix/strix.git
# already have the repo? check out this version:
$ git checkout v1.4.0
```

└──▷ TRY IT

Keep Strix up to date without reinstalling — run this after any release to pull the latest version in place.

```
$ strix --update
```

After a scan finishes (Strix no longer auto-opens the viewer), inspect results in the local dashboard.

```
$ strix view my-run-name
```

- Adds `strix --update` command for in-place CLI self-update and automatic update notifications.
- Supports signing in with a ChatGPT subscription as an inference provider.
- Adds Linux ARM64 standalone release builds.
- Enables AWS Bedrock/Anthropic prompt caching for Claude models to reduce latency and cost on repeated context.
- Adds a dedicated deduplication model to reduce duplicate findings across scan runs.

+5 more

└──▷ BREAKING ON UPGRADE

! Strix now quits after a scan completes instead of hosting a local viewer — workflows that relied on the viewer launching automatically must now run `strix view` separately.

WAS THIS USEFUL? 👍 👎

◆ Wireless & RF

multimon-ng ⓘ 1.6.0 NOTES ↗

Multimon-ng decodes and displays digital radio signals including POCSAG, DTMF, and other modes from audio input or SDR receivers.

multimon-ng 1.6.0 adds GSC paging, FLEX/POCSAG generation, macOS audio capture, SDL3 scope, and JSON output for GSC and `FLEX_NEXT`.

└──▷ GET THIS VERSION

```
$ git clone --branch 1.6.0 https://github.com/EliasOenal/multimon-ng.git
# already have the repo? check out this version:
$ git checkout 1.6.0
```

└──▷ TRY IT

Decode a live RTL-SDR feed for GSC paging traffic alongside `FLEX_NEXT`, capturing both with JSON-structured output for downstream parsing.

```
$ rtl_fm -f 929612500 -s 22050 | multimon-ng -t raw -a GSC -a FLEX_NEXT /dev/stdin
```

Generate a POCSAG test signal and a FLEX test signal using gen-ng to validate your receive chain or feed a decoder under test.

```
$ gen-ng -P "Test page message" -A 1234567 -B 1200 -t raw - | multimon-ng -t raw -a POCSAG1200 -
```

Replay a recorded FLAC capture through `FLEX_NEXT` with automatic input format detection to extract reassembled multi-frame messages with timestamps.

```
$ flac -d --stdout ~/recordings/rtlfm.1725033204.flac | multimon-ng -r -v 0 -a FLEX_NEXT -t flac -
```

- Adds GSC (Golay Sequential Code) paging decoder with error correction, auto-polarity, batch message support, and JSON output.
- Adds `FLEX_NEXT` decoder improvements based on ARIB STD-43A: more robust decoding, message reassembly, validation, timestamps, and JSON output.

- Adds FLEX and POCSAG signal generation via the new `gen-ng` binary.
- Adds native macOS audio capture support.
- Adds automatic input format detection.

+2 more

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

Codacy ⓘ

Adding PHP CS Fixer and support to Checkov configuration files July, 2026

NOTES ↗

Codacy is an automated code quality and security analysis platform that reviews pull requests, enforces coding standards, and tracks technical debt across repositories.

Codacy adds PHP CS Fixer as a new tool and gains support for Checkov configuration files.

- Adds PHP CS Fixer as a supported static analysis tool for PHP code style enforcement.
- Adds support for Checkov configuration files, enabling repository-level Checkov settings to be recognized by Codacy.

WAS THIS USEFUL? 👍 👎

Promptfoo ⓘ snapshot-20260727 NOTES ↗

Promptfoo is an open-source tool for testing, evaluating, and red-teaming LLM applications to detect vulnerabilities, improve reliability, and compare model outputs.

Promptfoo snapshot-20260727 adds adaptive rate limiting, Transformers.js local inference, telecom red team plugins, and video generation providers.

└──▷ **TRY IT**

Load multiple environment files (e.g., base secrets plus environment-specific overrides) in a single eval run.

```
$ promptfoo eval --env-file .env.base --env-file .env.staging
```

View Promptfoo service logs directly from the CLI instead of hunting through log directories.

```
$ promptfoo logs
```

- Adds Transformers.js provider to run Hugging Face models locally in Node.js or browser.
- Adds Vercel AI Gateway and Cloudflare AI Gateway providers for routing requests.
- Adds AWS Bedrock Video (Nova Reel, Luma Ray 2) and Azure AI Foundry Video (Sora) for video generation.
- Adds native session endpoint support to the HTTP provider for stateful conversations.
- Adds xAI Voice provider overrides for `apiBaseUrl`, `websocketUrl`, and function call support.

+22 more

WAS THIS USEFUL? 👍 👎

Veracode ⓘ Package Firewall updates (2026-07-07) BLOG ↗

Veracode is a cloud-based application security platform that helps developers identify and remediate vulnerabilities in their code through static, dynamic, and software composition analysis.

Veracode Package Firewall launches with automatic blocking of untrusted packages, now available in the European region.

- New Package Firewall service automatically blocks untrusted packages that don't comply with policies across artifact repositories and package managers.
- Package Firewall mitigates risks from malware, typosquatting, and license violations by enforcing verified, compliant dependencies.
- Package Firewall is now available in the European region.

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

Wapiti ⓘ 3.3.1 NOTES ↗

Web vulnerability scanner written in Python3

Wapiti 3.3.1 adds stacktrace disclosure detection, stronger SQL boolean-based detection, improved CSP analysis, and per-host passive reporting.

└──▷ GET THIS VERSION

```
$ git clone --branch 3.3.1 https://github.com/wapiti-scanner/wapiti.git
# already have the repo? check out this version:
$ git checkout 3.3.1
```

└──▷ TRY IT

Run passive modules (including the new stacktrace and CSP checks) against a target to surface disclosure issues without active fuzzing.

```
$ wapiti -u https://example.com -m csp,http_headers,cookieflags
```

Run boolean-based SQL injection detection (now robust to dynamic pages) alongside time-based SQL for comprehensive coverage.

```
$ wapiti -u https://example.com -m sql,timesql
```

- Adds passive detection of server-side stacktrace disclosures in HTTP responses.
- Improves boolean-based SQL injection detection to remain robust against dynamic/randomized pages.
- Enhances the passive CSP module to flag unknown directives and missing `frame-ancestors` and `form-action` directives.
- Reports distinct passive security postures per host, enabling per-target analysis across multi-host scans.
- Surfaces previously suppressed passive alerts in scan reports so no passive finding is silently dropped.

+3 more

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

iLEAPP ⓘ v2026.2.1 NOTES ↗ CODE ↗

iOS Logs, Events, And Plist Parser

iLEAPP v2026.2.1 adds 60+ Biome streams, full Signal for iOS parsing, expanded keychain handling, and notifications overhaul.

└──▷ GET THIS VERSION

```
$ git clone --branch v2026.2.1
https://github.com/abrignoni/iLEAPP.git
# already have the repo? check out this version:
$ git checkout v2026.2.1
```

└──▷ TRY IT

Supply an examiner-provided keychain file alongside an iTunes backup to enable keychain lookups across the new artifacts.

```
$ ileapp -t itunes -i /path/to/backup/ -o /path/to/output/ --
itunes_password <password>
```

- Adds 60+ new Biome artifact streams covering device power/lock state, location visit, app location activity, camera AutoFocus ROI, energy mode, boot session, emergency voice calls, emoji engagement, Device.Timezone, Wallet transactions, Siri Remembers Message/Audio History, Discoverability Signals, Siri UI, Siri suggestions, and a full Apple Intelligence family including Safety Overrides.
- New Signal for iOS support: full message and contact parsing, conversation view with attachments, and detection of Signal's timestamped GRDB directories.
- Expanded keychain handling: accepts examiner-supplied keychain input, adds a lookup helper, includes a pure-Python SQLCipher reader, supports UFED encrypted keychain dumps, and can reuse a keychain already present in the extraction.
- Notifications overhaul: attachments now checked in as media, images embedded in notification payloads recovered, and payload fields split into dedicated columns.
- Adds Notes – Password Protected artifact for password hint and recoverability triage.

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Runtime Security

NVIDIA OpenShell ⓘ v0.0.92 NOTES ↗

OpenShell is the safe, private runtime for autonomous AI agents.

OpenShell v0.0.92 adds JSON/YAML output for sandbox commands and corporate HTTP proxy egress routing.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.0.92 https://github.com/NVIDIA/OpenShell.git
# already have the repo? check out this version:
$ git checkout v0.0.92
```

└──▷ TRY IT

Pipe sandbox status into jq or other tooling by requesting JSON output — useful in CI pipelines or scripted workflows.

```
$ openShell sandbox status --output json | jq '.state'
```

Capture newly created sandbox details in YAML for audit logging or config-as-code workflows.

```
$ openShell sandbox create --output yaml > sandbox-record.yaml
```

- Adds `--output json` and `--output yaml` flags to `sandbox get`, `sandbox status`, and `sandbox create` commands for machine-readable output.
- Supports routing sandbox egress traffic through a corporate HTTP proxy via the gateway.

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Threat Intelligence

Feedly Threat Intelligence ⓘ changelog · Jul 27, 2026

CHANGELOG ↗

Feedly Threat Intelligence is a security tool that aggregates and analyzes threat feeds, helping security teams track emerging threats, vulnerabilities, and adversary activity in real time.

Feedly Ask AI gains SPL query generation and an improved threat actor campaign detection model alongside KQL support.

└──▷ HOW TO FIND IT

Generate a Splunk SPL hunting query for a specific threat actor campaign directly from Ask AI instead of switching to an external query builder.

> 📍 In the Feedly console, open Ask AI and prompt: "Generate an SPL hunting query for [threat actor] campaigns targeting [industry]."

- New Ask AI model tuned specifically for threat actor campaign detection.
- Adds SPL (Splunk Processing Language) hunting query generation to Ask AI, complementing existing KQL support.
- Improves MITRE ATT&CK tagging accuracy in Ask AI results.

WAS THIS USEFUL? 👍 👎

◆ SOAR

Tines ⓘ changelog · Jul 27, 2026 CHANGELOG ↗

Tines is a no-code automation platform that helps security and operations teams build workflows to automate repetitive tasks and incident response processes.

Tines 42.2.0 adds API key creation restrictions and template-based case creation via API.

- Adds the ability to restrict which users can create API keys.
- Enables creating cases from a template via the API.

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

Trend Vision One ⓘ

Endpoint Event Viewer enhancements and fixes (2026-07-27)

3 RELEASES · 2026-07-22 → 2026-07-27 BLOG ↗ LATEST STABLE

Trend Vision One is a unified cybersecurity platform that integrates extended detection and response (XDR) across endpoints, networks, email, and cloud environments.

Endpoint Event Viewer gains Event name and Event ID filtering in the System events view.

└──▷ HOW TO FIND IT

Narrow down System events to a specific Windows Event ID during an investigation without manually scrolling through all events.

📍 In the console, go to Endpoint Security → Endpoint Event Viewer, select the System events view, and use the Event name or Event ID filter to scope results.

› Adds filtering by Event name and Event ID in the Endpoint Event Viewer System events view.

▾ 2 more releases in this issue · 2026-07-22 → 2026-07-27

Zero Trust Secure Access On-premises Gateway version 1.0.89 (2026-07-27)

BLOG ↗ STABLE

Zero Trust Secure Access On-premises Gateway 1.0.89 adds Microsoft Tenant Restriction v1 support in AI Secure Access rules.

› Supports Microsoft Tenant Restriction v1 in AI Secure Access rules, enabling organizations to restrict AI service access to approved Microsoft tenants.

Helm Chart 3.5.0 (2026-07-22) BLOG ↗ STABLE

Helm Chart 3.5.0 upgrades Falco to 0.43.0 and adds OpenShift platform override control via values.yaml

└──▷ USE IT

Force OpenShift mode on or off when auto-detection is unreliable in your cluster environment.

```yaml
openshift:
  enabled: true
```

Upgrade an existing deployment to Helm Chart 3.5.0 with your local overrides.

```
$ helm upgrade \
  --values overrides.yaml \
  --namespace trendmicro-system \
  trendmicro \
  https://github.com/trendmicro/visionone-container-security-
helm/archive/3.5.0.tar.gz
```

- Upgrades Falco to 0.43.0, Falco libs to 0.23.1, and plugins to v0.7.1 with updated falco.yaml plugin configuration.
- Adds `openshift.enabled` field in values.yaml to explicitly override OpenShift platform auto-detection in unreliable environments.
- Skips the `api-server-modifier` DaemonSet and its ClusterRole on OpenShift, where the kube-apiserver is operator-managed.
- Reduces Scan Manager to least-privilege RBAC on non-OpenShift clusters by removing OpenShift-specific permissions.

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

Intruder ⓘ changelog · Jul 27, 2026 CHANGELOG ↗

Intruder is a cloud-based vulnerability scanner that continuously monitors and identifies security weaknesses in internet-exposed systems, APIs, and web applications.

Intruder extends Azure cloud scans to cover Microsoft 365 configuration risks across Entra, Exchange, SharePoint, and Teams.

└──▷ HOW TO FIND IT

Unlock full Microsoft 365 configuration checks — beyond the automatic subset — by updating your Azure integration's permissions in Intruder.

> 📍 In the Intruder console, go to your Azure integration settings and update the integration's permissions following the steps outlined in the integration guide to enable the full set of M365 checks.

- Adds Microsoft 365 configuration risk scanning (Entra ID, Exchange Online, SharePoint, Teams) as part of existing Azure cloud security scans.
- Surfaces M365 identity, email, and collaboration configuration risks automatically for existing Azure integration users.
- Enables full M365 check coverage by updating the Azure integration's permissions.

WAS THIS USEFUL? 👍 👎

◆ Vulnerability Management

defectdojo ⓘ 3.1.300 NOTES ↗

Open-Source Unified Vulnerability Management, DevSecOps & ASPM

DefectDojo 3.1.300 adds a Fortify parser v2, tighter API permission controls, and a case-insensitive index on Vulnerability ID.

└──▷ GET THIS VERSION

```
$ git clone --branch 3.1.300 https://github.com/DefectDojo/django-DefectDojo.git
# already have the repo? check out this version:
$ git checkout 3.1.300
```

- New Fortify parser v2 prefers true source line numbers for more accurate finding location reporting.
- Adds case-insensitive expression index on `Vulnerability_Id.vulnerability_id` for faster, case-insensitive vulnerability lookups.
- Restricts configuration permission assignment to superusers only in the user API, tightening privilege escalation controls.
- Scopes location and endpoint reference writes to authorized products, enforcing product-level authorization on those API writes.
- Extends user serializer validation to identity and permission fields for stricter input validation.

+1 more

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Castle ⓘ Detect VPN traffic with new IP intelligence

4 RELEASES · seen 2026-07-27 NOTES ↗ LATEST STABLE

Castle is a security platform that helps developers detect and block account takeover, fraud, and bot attacks in real time.

Castle adds VPN traffic detection via new IP intelligence signals.

› Detects VPN traffic using new IP intelligence, extending existing tunnel and residential proxy detection capabilities.

▾ 3 more releases in this issue · seen 2026-07-27

Detect residential proxies with new IP intelligence NOTES ↗ STABLE

Castle adds Residential Proxy IP signal and richer IP tunnel intelligence to its IP risk detection.

› New Residential Proxy IP signal detects traffic routed through real consumer ISPs, catching proxies invisible to traditional datacenter-based detection.

› Expanded IP tunnel intelligence provides richer context alongside existing Proxy IP and Tor IP signals.

Export team members to CSV NOTES ↗ STABLE

Castle lets you export your team members list to CSV from Team Settings for access reviews and compliance audits.

└──▷ HOW TO FIND IT

Pull an offline team roster for a periodic access review or compliance audit.

📍 In the Castle console, go to Settings › Team, then click the Export to CSV button to download all visible columns (name, email, user role, 2FA status, member since).

› Export team members list to CSV from the Team Settings page, including name, email, user role, 2FA status, and member-since date.

New event field: `email.registered_domain` NOTES ↗ STABLE

Castle adds `email.registered_domain` field to collapse subdomain variants for better fraud detection.

› Adds `email.registered_domain` event field that strips subdomains down to the registered domain using the public suffix list, making it easier to detect fraud

> patterns that rotate across subdomains.

WAS THIS USEFUL? 👍 👎

JumpCloud ⓘ

JumpCloud Agent Release Notes for July 27, 2026 (2026-07-27) BLOG ↗

JumpCloud is a cloud-based directory platform that manages user identities, devices, and access to applications and networks across organizations.

JumpCloud Agent 2.149.3 expands tray/menu bar app visibility and refines Self Service App Catalog display.

- Windows tray app and macOS menu bar app now visible to users with local or Google password sources when the Self Service App Catalog is enabled.
- Self Service App Catalog now filters to show only Winget (Windows) and macOS JumpCloud App Catalog apps, removing unsupported package manager types.

WAS THIS USEFUL? 👍 👎

Auth0 ⓘ

Cross App Access (XAA) for Resource Applications is now in Open Early Access (2026-07-27)

BLOG ↗

Auth0 is a cloud-based identity platform that provides authentication and authorization services, enabling developers to securely add login and access control to applications.

Auth0 launches Cross App Access (XAA) for Resource Applications in Open Early Access, enabling secure agent-to-app and app-to-app authorization.

- Adds Cross App Access (XAA), a new open standard for passing authorization across domains, enabling AI agents and enterprise apps to securely access MCP servers and APIs without per-user consent prompts.
- Centralizes IT control over cross-application data-sharing connections, improving governance and visibility into which agents and apps access which resources.
- Supports SAML and OIDC enterprise IdPs — including specific support for Okta — with no code changes required on the resource application side.
- Available in production at no additional cost for Enterprise, B2B Pro, and B2B Essential customers via Auth0 Enterprise Connections; Free tenants can test it during the trial period.

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

OpenAI Codex CLI ⓘ rust-v0.146.0-alpha.13 NOTES ↗ CODE ↗

PRE-RELEASE

Lightweight coding agent that runs in your terminal

Codex CLI alpha.13 adds cached MCP tool exposure before server startup and model-owned token budget defaults.

└──▷ GET THIS VERSION

```
$ git clone --branch rust-v0.146.0-alpha.13
https://github.com/openai/codex.git
# already have the repo? check out this version:
$ git checkout rust-v0.146.0-alpha.13
```

- Exposes cached MCP tools to inference before the MCP server finishes initializing, reducing latency at session start.
- Supports model-owned token budget defaults from the model catalog, applied automatically when no explicit token-budget configuration is set.

WAS THIS USEFUL? 👍 👎

AGENT

◆ AI Agent Frameworks

CrewAI ⓘ 1.15.7 2 RELEASES · 2026-07-26 NOTES ↗ LATEST STABLE

Framework for orchestrating role-playing, autonomous AI agents. By fostering collaborative intelligence, CrewAI empowers agents to work together seamlessly, tackling complex tasks.

CrewAI 1.15.7 adds runtime skill usage event emission for observability.

└──▷ GET THIS VERSION

```
$ git clone --branch 1.15.7 https://github.com/crewAIInc/crewAI.git
# already have the repo? check out this version:
$ git checkout 1.15.7
```

› Emits skill usage events at runtime, enabling observability pipelines to trace which skills agents invoke during execution.

▾ 1 more release in this issue · 2026-07-26

1.15.7a1 NOTES ↗ PRE-RELEASE

CrewAI 1.15.7a1 adds runtime skill usage event emission for improved observability.

└──▷ GET THIS VERSION

```
$ git clone --branch 1.15.7a1
https://github.com/crewAIInc/crewAI.git
# already have the repo? check out this version:
$ git checkout 1.15.7a1
```

› Emits skill usage events at runtime, enabling observability pipelines to track which skills agents invoke during execution.

WAS THIS USEFUL? 👍 👎

DEPLOY

◆ Local LLM Runtimes

vMLX ⓘ v1.6.16 NOTES ↗

vMLX - JANGTQ Uber Compressed MLX Models - L2 Disk Cache (survives restart) + L1 Paged (super fast ttft) + Hybrid SSM Scheduler + Cont Batching + etc!

vMLX 1.6.16 ships KaTeX-backed Electron renderer for chat and reasoning surfaces and hardens bundled engine provenance.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.6.16 https://github.com/jjang-ai/vmlx.git
# already have the repo? check out this version:
$ git checkout v1.6.16
```

- Adds KaTeX-backed Electron renderer path for chat and reasoning surfaces.
- Hardens packaged engine provenance so signed app sessions use bundled Python/vmlx_engine instead of stale development or system virtualenvs.

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

AI-Infra-Guard ⓘ v4.5.0 NOTES ↗

A full-stack AI Red Teaming platform securing AI ecosystems via OpenClaw Security Scan, Agent Scan, Skills Scan, MCP scan, AI Infra scan and LLM jailbreak evaluation.

AI-Infra-Guard v4.5.0 adds standalone CLI modules for Agent/MCP/Skill scanning, new AI agent detection skills, SARIF output, and open-source frontend.

└──▷ GET THIS VERSION

```
$ git clone --branch v4.5.0 https://github.com/Tencent/AI-Infra-Guard.git
# already have the repo? check out this version:
$ git checkout v4.5.0
```

- Modularizes Agent-Scan as a standalone CLI with AIG integration support, adding 4 new AI agent security detection skills.
- Modularizes MCP-Scan with dual-mode support (CLI + AIG Web) and adds a standalone mcp-scan-lite module.
- Adds 2 new MCP security detection rules plus ATR-derived MCP detection rules covering additional attack surfaces.
- Adds Agent Skill security auditing (Skill-Scan) repackaged as the standalone PyPI package `aig-skill-scan`.
- Adds SARIF 2.1.0 output format for Skill-Scan results alongside single-stage optimization.

+4 more

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

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

▷ Subscribe