THE CYBER TOOLCHAIN NO. 004

Head

THE WEEK'S TOP PICKS

PUBLISHED JULY 24, 2026 · FRIDAYS

// SHARE THIS WEEK ▽ Top 5 ▽ Top Pick

The best tooling updates that shipped this week.

// HOW THESE PICKS ARE MADE

Every feature release from the 874 tools on our watchlist goes into the daily newsletter. Once a week we read the whole field side by side and pick the few updates worth your attention, on two questions: **how deep and complete is the single best capability in the release**, and **how much it changes what you can actually do**.

A tool is judged on everything it shipped that week, so a project that releases daily gets credit for the sum — and still only takes one slot. We would rather run a short list than a padded one.

// THE PICKS

01	**VulnHunter**	SAST / SCA / Code Security
02	**noir**	SAST / SCA / Code Security
03	**Pomerium**	Secure Access (VPN / SASE / ZTNA)
04	**Grype**	Container & Image Security
05	**Wiz Defend**	Runtime Security

01 VulnHunter

1 RELEASE · 2026-07-18

SAST / SCA / Code Security

Agentic AI security tool that applies proactive, attacker-first analysis directly to source code.

// WHY IT MADE THE LIST

DEPTH 5/5 IMPACT 5/5

Capital One open-sourced VulnHunter, an agentic SAST that maps attacker paths to dangerous sinks and filters findings through a multi-stage falsification pipeline, then runs a test-driven fix loop that writes a failing security test, implements the fix, verifies the exploit is blocked, and opens a reviewable PR. A headless CI/CD runtime and batch benchmarking harness make it deployable beyond the desktop.

> Capital One open-sourced VulnHunter v0.1.0, an agentic AI SAST tool built around an attacker-first scanning skill, a falsification pipeline, an automated fix-and-verify loop, and both a CI/CD-ready headless runtime and a batch-scanning harness.

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

01 Attacker-first scanner via /vulnhunt skill NEW

95

The `/vulnhunt` Claude Code skill is an entry-point-forward scanner that maps attacker paths to dangerous sinks and filters findings through a multi-stage falsification pipeline: Recon → Parallel Hunt → Adversarial Disprove → Capability Filter. It is run inside a Claude Code session via `claude --model opus --add-dir ~/.claude/skills/vulnhunt --add-dir ~/.claude/skills/vulnhunt/phases` followed by `/vulnhunt`.

Run the full attacker-first vulnerability scan against a codebase inside a Claude Code session.

```
$ claude --model opus --add-dir ~/.claude/skills/vulnhunt --add-dir ~/.claude/skills/vulnhunt/phases
# Then inside the Claude Code session:
/vulnhunt
```

— Names full pipeline stages and gives a runnable command v0.1.0

02 Independent fix verification via /vulnhunt-fix-verify NEW

90

The `/vulnhunt-fix-verify` skill is an independent, read-only agent that validates whether a finding was successfully remediated and emits a per-finding verdict. It is invoked with `claude --model opus --add-dir ~/.claude/skills/vulnhunt-fix-verify --add-dir ~/.claude/skills/vulnhunt-fix-verify/phases` then

`/vulnhunt-fix-verify repo=<abs_path> report=<abs_path> fixed=VULN-001,... out=<abs_path>`.

Independently verify that a prior fix actually blocked the exploit before merging, using the read-only verifier agent.

```
$ claude --model opus --add-dir ~/.claude/skills/vulnhunt-fix-verify \
       --add-dir ~/.claude/skills/vulnhunt-fix-verify/phases
# Then inside the Claude Code session:
/vulnhunt-fix-verify repo=<abs_path> report=<abs_path>
fixed=VULN-001,... out=<abs_path>
```

— Exact runnable command with argument names provided `v0.1.0`

---

03 **Batch scanning and benchmarking harness** NEW 90

The `harness/` tooling manages a repo list, resumes interrupted scans, collects findings centrally, and evaluates detection accuracy against a known-vulnerable corpus using LLM-judge scoring. It is run via `cd harness`, `python -m local_harness.batch.run scan --resume`, and `python -m local_harness.batch.run collect`.

Batch-scan a list of repositories and collect all findings for centralized review, skipping repos already processed.

```
$ cd harness
python -m local_harness.batch.run scan --resume
python -m local_harness.batch.run collect
```

— Concrete runnable commands for scanning and collecting results `v0.1.0`

---

04 **Test-driven remediation via /vulnhunter-fix skill** NEW 70

The `/vulnhunter-fix` skill runs a test-driven remediation loop: it writes an exploit demo, creates a failing security test (RED), implements the fix (GREEN), verifies the exploit is blocked, and opens a reviewable PR.

— Mechanism (RED/GREEN loop) described but no invocation example `v0.1.0`

---

05 **Headless CI/CD scanning runtime** NEW 60

The `vulnhunter-agent/` headless runtime clones target repositories, runs `/vulnhunt`, publishes results, and opens GitHub issues for confirmed vulnerabilities, making it suitable for use in CI/CD pipelines.

— Workflow described but no concrete command or config shown `v0.1.0`

GOOD PICK? 👍 👎 GOOD REASON? 👍 👎

02 noir

1 RELEASE · 2026-07-19

SAST / SCA / Code Security

Hunt every Endpoint in your code, expose Shadow APIs, map the Attack Surface.

// WHY IT MADE THE LIST

DEPTH 5/5 IMPACT 4/5

Noir now detects CLI application attack surfaces (argv, flags, env vars) across 17 languages, and adds schema-driven API analyzers, built-in HTTP server detection, enterprise legacy stacks (ColdFusion, Classic ASP, WebForms), and order-of-magnitude performance gains. It substantially widens what an attack-surface mapper can enumerate before a scan.

> Noir v1.2.0 adds CLI application attack-surface detection and dramatically expands endpoint discovery across new stdlib HTTP servers, schema-driven CMS/backend platforms, enterprise legacy stacks, Terraform IaC, and realtime protocols, alongside a redesigned HTML report and order-of-magnitude performance gains.

└──▷ WHAT SHIPPED · 14 FEATURES most completely described first ? what's the number?

01 Terraform/OpenTofu API Gateway route extraction NEW

73

Adds a Terraform/OpenTofu analyzer that extracts AWS API Gateway v1/v2 routes from `.tf` HCL and `.tf.json` files, resolved module-wide.

— Names file types and module-wide resolution mechanism v1.2.0

02 Major performance improvements across scanners IMPROVED

73

A codebase-wide performance sweep eliminates O(n²) scans, adds precompiled regex unions, and memoizes tree-sitter results, delivering order-of-magnitude speedups — e.g., F#/Giraffe scanning dropped from 31.7s to 1.1s, and Servant from 101s to 4ms.

— Concrete before/after numbers and mechanism, but not user-actionable v1.2.0

03 Redesigned HTML report output IMPROVED

70

The `-f html` report format is redesigned with a dark-tech theme, semantic method/severity colors, path grouping, a table view, and copy URL/curl actions.

— Exact flag given plus concrete UI features v1.2.0

04 CLI application surface detection NEW

65

Noir now detects CLI application attack surfaces — argv arguments, flags, and environment variables — across 17 languages and 40+ CLI libraries, including Cobra,

Click, clap, Commander, Thor, and picocli.

— Mechanism and scope named, but no invocation flag given v1.2.0

05 **Machine-readable `noir list` output and `noir cache purge`** NEW

65

Adds machine-readable output for `noir list` and documents the `noir cache purge` subcommand.

— Exact runnable subcommands named v1.2.0

06 **Built-in HTTP server analyzers for 9 languages** NEW 60

Adds analyzers for core/stdlib HTTP servers: Go's `net/http`, Python's `http.server`, Node's `node:http`, Java's `com.sun.net.httpserver`, C#'s `HttpListener`, Ruby's WEBrick, plus Crystal, Dart, and Zig.

— All targets named but detection is automatic, no explicit usage v1.2.0

07 **Schema-driven API analyzers for CMS/backend platforms** NEW

60

Adds analyzers for Strapi, Directus, Payload CMS, Supabase/PostgREST, Hasura, and Appwrite that extract routes and params from schema files rather than source-code routes.

— Names mechanism (schema files) and all six platforms v1.2.0

08 **PHP CMS/platform analyzers (WordPress, Drupal, Magento)** NEW

60

Adds analyzers for WordPress (REST API, admin-ajax, admin-post), Drupal (`*.routing.yml`), and Magento (Web API + MVC controller routes).

— Names concrete surfaces like `*.routing.yml` and admin-ajax v1.2.0

THINNER COVERAGE BELOW

09 **Enterprise legacy stack support (CFML/ASP)** NEW 50

Adds support for CFML/ColdFusion, Classic ASP, and ASP.NET WebForms, plus CFML frameworks Taffy, ColdBox, Wheels, and FW/1.

— Lists all stacks and frameworks but no mechanism detail v1.2.0

10 **OpenRPC and `.http`/`.rest` file analyzers** NEW 50

Adds specification analyzers for OpenRPC and `.http` / `.rest` request files used by VS Code REST Client and JetBrains HTTP Client.

— Names formats and tools they originate from v1.2.0

11 **Realtime/event endpoint detection** NEW 45

Adds detection for realtime/event endpoints in SignalR, Socket.IO, Phoenix Channels, and Action Cable.

— Names four frameworks but no mechanism detail v1.2.0

12 **BEAM language support (Erlang, Gleam)** NEW 35

Adds BEAM language support for Erlang (Cowboy, Elli) and Gleam (Wisp).

— Bare list of two languages and their libraries v1.2.0

13 **New AI providers added to token map** NEW 35

Adds Claude Sonnet 5, Grok 4.5, and GPT-5.6 to the AI provider token map.

— Just a list of added provider names v1.2.0

14 **Django Ninja and Plumber framework analyzers** NEW 30

Adds framework analyzers for Django Ninja (Python) and Plumber (R).

— Two names, no further detail given v1.2.0

GOOD PICK? 👍 👎 GOOD REASON? 👍 👎

03 Pomerium

8 RELEASES · 2026-07-23

Secure Access (VPN / SASE / ZTNA)

Pomerium is an identity-aware proxy that provides secure, clientless access to internal applications by enforcing context-based authentication and authorization policies.

// WHY IT MADE THE LIST

DEPTH 5/5 IMPACT 4/5

Pomerium Enterprise adds SSH session recording that captures every keystroke and terminal output for privileged connections, stored in portable asciicast format on any S3-compatible bucket with a Console playback UI. Native SSH also gains OAuth Authorization Code login, reverse tunnels, and jump-host mode, plus a 'revoke and block' incident-response option.

> Pomerium's biggest window pairs enterprise SSH session recording with a major native-SSH overhaul — a switch to OAuth Authorization Code auth, reverse tunnels, jump-host mode and a routes portal — alongside deeper upstream OAuth support for the MCP gateway, a new hosted identity provider, stronger session revocation, and Databroker/DNS performance work.

└──▷ WHAT SHIPPED · 11 FEATURES most completely described first ? what's the number?

01 Reverse tunnels, jump-host mode, and routes portal for native SSH

NEW

95

The `ssh_upstream_tunnel` flag lets upstream SSH servers dial out to Pomerium, useful for edge devices, NAT'd networks, and isolated environments, and Pomerium policy now supports these upstream SSH tunnels. The `ssh_allow_direct_tcpip` flag enables jump-host (ProxyJump) mode so clients can tunnel through Pomerium to an upstream without the upstream trusting Pomerium's User CA. The `ssh_routes_portal` flag presents an interactive picker of authorized destinations when a client SSHes to Pomerium without specifying a route.

Enable reverse tunneling so SSH servers behind NAT or on edge networks can dial out to Pomerium and receive authorized inbound sessions.

yaml

```yaml
ssh_upstream_tunnel: true
```

Enable jump-host (ProxyJump) mode so clients can tunnel straight through Pomerium to an upstream SSH server without requiring the upstream to trust Pomerium's User CA.

```yaml
ssh_allow_direct_tcpip: true
```

Enable the interactive routes portal so users who SSH to Pomerium without specifying a route get a picker of all destinations they're authorized to reach.

```yaml
ssh_routes_portal: true
```

— Three exact YAML flags with runnable snippets for each mode.

Native SSH: Authorization Code Flow, Rev…

---

02 **SSH session recording and playback** NEW 85

Enterprise now captures every keystroke and terminal output for privileged SSH connections and replays it directly from the Console. Recordings can be stored on a local on-disk directory or any S3-compatible bucket, configured per cluster, with a blob-URI builder in the Console (supporting Go CDK driver options and advanced parameters) so admins don't hand-write connection strings. A new Recordings UI lets teams browse, sort, and filter sessions by route, SSH user, target host, duration, and size, and recordings are stored in the open, portable asciinema (.asciicast) format.

Review a full audit trail of a privileged SSH session after the fact — filter by user or host, then replay terminal output.

> 📍 In the Enterprise Console, go to Recordings, filter by SSH user or target host, select a session, and click Play to replay the recorded terminal output.

— Names storage options, UI filters and file format concretely.

SSH Session Recording (Enterprise)

---

03 **Upstream OAuth authentication for MCP routes** NEW 81

Pomerium discovers upstream OAuth metadata, completes authorization flows, caches client and token state, and injects upstream access tokens into MCP traffic, using SSRF-safe metadata fetching with path-prefix validation. It includes the `iss` parameter in authorization flows (returning Pomerium's host as issuer, aligning with the 2026-07-28 MCP spec) and enables auto-discovery for MCP connect, disconnect, and authorize endpoints. Dynamic Client Registration via client ID metadata documents acts as a fallback for tools like MCP Inspector that lack that support, and OAuth refresh tokens keep long-running AI agents and clients connected without repeated interactive logins. Also adds proactive upstream token refresh before forcing reauthentication, upstream auth recovery after late config delivery, clearer errors when upstream tokens can't be resolved, customizable MCP 401 error pages, an optional allowed-client-domains

setting, and a proper WWW-Authenticate header on unauthorized responses; the routes portal now shows server indicators and connect/disconnect controls for MCP routes.

— Names many endpoints and mechanisms but no runnable command.

MCP: Refresh Tokens, Dynamic Client Regi… | MCP: Upstream OAuth, Dynamic Client Regi…

---

04 **Revoke and block future authentication for sessions** NEW

75

Enterprise session revocation gains a 'Revoke and block future authentication' option that prevents SSO re-authentication loops after revocation, enforced via a deny/revocation list so blocked users are rejected on all subsequent requests, not just the current session.

During an incident response, permanently lock out a compromised user so they cannot silently re-authenticate through SSO after session revocation.

> 📍 In the Enterprise Console, go to Sessions, find the target user's session, open the revocation dialog, and select 'Revoke and block future authentication'.

— Names the mechanism and gives exact UI navigation steps.

Revoke and Block: Stronger Session Revoc…

---

05 **Databroker indexing, query engine, and Pebble storage** NEW

75

Introduces Databroker indexing and query support, including field-based record lookup, a new `GetOptions` API, additional filter operators, and order-by. Replaces the in-memory store with Pebble, aligning it with the persistent backend and setting a default path for the file backend. Sync gains a 'latest stream' option and safely aborts calls with invalid record versions, improving resilience for large deployments.

— Names the API and storage engine but no exact usage command.

Faster Config Updates & a New Databroker…

---

06 **SSH authentication switched to OAuth Authorization Code flow**

68

BREAKING

Native SSH auth now uses the OAuth Authorization Code grant instead of Device Code, giving a faster browser login with full telemetry observability. This is breaking: upstream IdPs must have the Authorization Code grant enabled, since v0.31.x and earlier relied on Device Code, which is no longer used.

— Clear before/after and migration requirement, no exact config shown.

Native SSH: Authorization Code Flow, Rev…

---

07 **Hosted identity provider** NEW

66

A new hosted identity provider type lets Pomerium manage authentication without teams configuring an external OIDC provider. Built-in refresh handling authenticates session refresh requests and correctly hashes the derived IdP configuration for clean session renewal.

Enable the Pomerium-hosted IdP as your identity source instead of wiring up an external OIDC provider — ideal for evaluations or small deployments.

> 📍 In the Pomerium console, go to Settings › Identity Provider and select the Pomerium-hosted IdP as your identity source.

— Explains mechanism and gives UI path to enable it. `Hosted Identity Provider`

---

08 **MCP tool library for Pomerium config service** NEW 65

Introduces a new `pkg/mcp/configapi` library that exposes Pomerium's ConfigService as MCP tools, with generated schemas, sensitive-field handling, and update-safety checks.

— Names the exact package and its safeguards. `MCP: Upstream OAuth, Dynamic Client Regi…`

THINNER COVERAGE BELOW

09 **Configurable DNS resolvers** NEW 55

Supports specifying custom DNS servers for resolving upstream routes, independent of the host system's resolver, and enables tunable DNS refresh rates so record changes are picked up on a schedule matching the environment, giving consistent, centrally configured name resolution across all Pomerium components for dynamic and clustered deployments.

— Describes capability and scope but no config key named. `Configurable DNS Resolvers`

---

10 **Per-key session management for native SSH** NEW 42

Adds per-key session management and revocation in the Pomerium UI, binding each SSH key to an OAuth user with policy evaluated on every connection.

— Describes the capability but no UI path or command given.

`Native SSH: Authorization Code Flow, Rev…`

---

11 **Incremental config diffing for routes** IMPROVED 42

Adds incremental config diffing for routes — only changed routes are recomputed and applied, reducing churn on large route sets.

— States the mechanism but no config surface or numbers.

`Faster Config Updates & a New Databroker…`

└──▷ BREAKING ON UPGRADE

! SSH authentication now uses the Authorization Code grant; upstream IdPs must have the Authorization Code grant enabled (v0.31.x and earlier used Device Code, which is no longer used).

GOOD PICK? 👍 👎 GOOD REASON? 👍 👎

04 Grype

1 RELEASE · 2026-07-16

Container & Image Security

A vulnerability scanner for container images and filesystems

// WHY IT MADE THE LIST

DEPTH 4/5 IMPACT 4/5

Grype adds Go symbol-based reachability analysis that suppresses false positives by flagging only binaries that actually import the vulnerable symbol, cutting noise on stdlib and third-party Go advisories. It also adds Ubuntu ESM matching and a Chainguard OSV transformer.

> Grype v0.116.0 adds Go symbol-based reachability analysis to cut false positives, plus broader distro coverage with Ubuntu ESM matching, a Chainguard OSV transformer, and more complete RHEL advisory duplication.

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

THINNER COVERAGE BELOW

01 Go symbol reachability analysis NEW

55

Adds lightweight Go symbol reachability analysis to suppress false positives for stdlib, golang.org/x, and third-party Go vulnerability advisories — it only flags binaries that actually import the vulnerable symbols.

– Explains mechanism but no user-facing flag or command given. v0.116.0

02 Go match deduplication for aliased advisories IMPROVED

45

Deduplicates Go matches that are aliases of each other, i.e. the same CVE reported under both a govulndb `GO-*` ID and its corresponding GHSA.

– Clear mechanism named but purely automatic, nothing to invoke. v0.116.0

03 Expanded RHSA coverage across RHEL versions IMPROVED

40

Duplicates RHSA advisories across all applicable RHEL minor versions for more complete RHEL vulnerability coverage.

– States the before/after improvement but no numbers or examples. v0.116.0

04 Chainguard OSV transformer NEW

35

Adds a Chainguard OSV transformer for processing Chainguard vulnerability data.

– Names the integration but not how it's used or configured. v0.116.0

05 **Ubuntu ESM vulnerability matching** NEW 25

Adds support for matching vulnerabilities against Ubuntu ESM (Extended Security Maintenance) data.

— Bare mention with no detail on scope or activation. v0.116.0

GOOD PICK? 👍 👎 GOOD REASON? 👍 👎

05 Wiz Defend

1 RELEASE · 2026-07-22

Runtime Security

Wiz Defend is a cloud detection and response platform that identifies and helps remediate real-time threats across cloud environments.

// WHY IT MADE THE LIST

DEPTH 4/5 IMPACT 4/5

Wiz Agentless Workload Detection now delivers EDR-like visibility into FortiGate appliances, Redis replication abuse, and npm supply-chain compromises by parsing local logs never streamed off the box, and ships detections for actively exploited CVEs including BeyondTrust CVE-2026-1731 and PAN-OS flaws.

> Wiz Defend extends Agentless Workload Detection with new visibility into FortiGate firewalls, Redis, npm supply chain activity, and web server access logs, plus fresh detection rules for several actively exploited CVEs.

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

01 Agentless threat visibility for FortiGate firewalls NEW

80

Extends Agentless Workload Detection to FortiGate appliances by collecting and parsing local FortiOS logs not typically streamed, exposing attacker activity such as super-user account creation and configuration theft. Adds Cloud Event page visibility for FortiGate authentication logs, enabling real-time monitoring of login activity and admin account changes for agentless EDR customers.

Hunt for rogue admin account creation on FortiGate devices during active CVE-2026-24858 exploitation — search the Cloud Event page for admin accounts named 'helpdesk'.

📍 In the Wiz console, go to Cloud Events and run the pre-built query to search for creation of an admin named 'helpdesk' on FortiGate devices.

Detect dangerously permissive FortiGate admin accounts (trusthost 0.0.0.0/0) that allow management access from any IP — a key persistence indicator in documented FortiGate campaigns.

📍 In the Wiz console, go to Cloud Events and run the pre-built event query to search for creation of admin accounts with trusthost set to 0.0.0.0/0 on FortiGate devices.

— Describes mechanism and includes exact Cloud Event query steps. 2026-07-22-ed8bb2c2

02 Redis replication abuse detection rules NEW

65

Adds built-in threat detection rules for Redis replication abuse: `Redis suspicious replication target configured`, `Redis module loaded from unusual path`, and `Attack Detected and Prevented by Redis`.

— Names all three rules but no usage walkthrough given. `2026-07-22-ed8bb2c2`

03 **Webshell and web access log visibility** NEW 60

Provides agentless visibility into HTTP/HTTPS access logs (Nginx, Apache, IIS) to detect webshell deployments, unusual executable access, and exploitation of hosted applications such as WordPress via the wp2shell webshell.

— Names three web servers and a specific webshell tool. `2026-07-22-ed8bb2c2`

04 **Detection coverage for actively exploited CVEs** NEW 60

Adds detection for PAN-OS `CVE-2026-0257` and `CVE-2026-0300` exploitation patterns, BeyondTrust Remote Support `CVE-2026-1731` (CVSS 9.9 pre-auth RCE), and MongoBleed `CVE-2025-14847`, an unauthenticated MongoDB memory leak, each observed in active exploitation and surfaced via agentless log ingestion with real-time alerting.

— Names four CVEs with CVSS score but no usage steps. `2026-07-22-ed8bb2c2`

THINNER COVERAGE BELOW

05 **npm supply chain log monitoring** NEW 50

Enables agentless monitoring of npm package installation logs to detect supply chain compromises, such as malicious versions of `@asyncapi/specs`, in real time.

— Names the example package but no concrete usage steps. `2026-07-22-ed8bb2c2`

06 **Correlation of agentless events with ASM findings** NEW 50

Correlates Agentless Workload events with Wiz ASM findings to surface threats like Zabbix instances running from unusual paths with default credentials.

— Gives one concrete example but no mechanism detail beyond correlation.

`2026-07-22-ed8bb2c2`

GOOD PICK? 👍 👎 GOOD REASON? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · This Week's Highlights · July 24, 2026
The full firehose — every feature release, every day — is in the newsletter.

▷ Subscribe