THE CYBER TOOLCHAIN

NO. 032

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED AUGUST 1, 2026 · EVERY DAY

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

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 26 tools

APPLICATION SECURITY

vim ? help

◆ Web Application Security

Invicti ⓘ changelog · Aug 1, 2026 CHANGELOG ↗

Invicti is an automated application security testing platform that identifies and reports vulnerabilities in web applications and APIs.

┗╾▷ HOW TO FIND IT

Enable AI-aided login recovery so scans can automatically recover from LSR playback failures without manual intervention.

> 📍 In the Invicti console, open your scan policy or scan settings, locate the AI-aided Login setting, and enable it.

- Adds AI-aided Login recovery: when an LSR playback fails during a scan, Invicti can now use AI to recover and complete authentication, reducing scan failures caused by login issues.
- Increases the character limit for authentication values in IDOR/BOLA credentials from 1,024 to 4,096 characters, enabling long JWT Bearer Tokens to be saved.

WAS THIS USEFUL? 👍 👎

humble ⓘ 1.64 NOTES ↗

A humble and fast security-oriented HTTP headers analyzer.

humble 1.64 adds multiple output format support, redirect totals in Info section, and an improved AI SKILL file.

└──▷ GET THIS VERSION

```
$ git clone --branch 1.64 https://github.com/rfc-st/humble.git
# already have the repo? check out this version:
$ git checkout 1.64
```



- Supports exporting analysis results in multiple output formats simultaneously via a single invocation.
- Shows the total number of redirects in the `Info` section of each analysis.
- Adds improved redirect information detail in analysis output.
- Adds 1 new fingerprint header detection to the fingerprint checks database.
- Greatly improved SKILL file for AI-assisted workflows.

WAS THIS USEFUL? 👍 👎

nikto ⓘ 2.6.1 NOTES ↗

Nikto web server scanner

Nikto 2.6.1 adds SQL Direct database reporting, TLS keep-alives for ~18% faster scans, and a new COOKIE: DSL matcher.

└──▷ GET THIS VERSION

```
$ git clone --branch 2.6.1 https://github.com/sullo/nikto.git
# already have the repo? check out this version:
$ git checkout 2.6.1
```

└──▷ TRY IT

Stream scan findings directly into a PostgreSQL database for centralized reporting across multiple scans.

```
$ nikto.pl -h https://target.example.com -o results -F sqld
```

- Adds `-F sqld` output format to insert findings directly into a MySQL or PostgreSQL database via the new SQL Direct plugin.
- TLS connections now use keep-alives for session reuse, delivering an ~18% scan speed increase; disable with `-nosslkeepalive` if a server misbehaves.
- Adds `-useragent` flag to force a specific User-Agent string for all requests.
- Adds `-evasion R` option for per-request random User-Agent rotation from the database.
- Adds `COOKIE:` and `!COOKIE:` DSL matchers to the test database for matching or excluding HTTP cookie content in custom rules.

+1 more

└──▷ BREAKING ON UPGRADE

- ! The dictionary attack plugin has been removed; scans relying on it will no longer function.
- ! User-Agent is no longer rotated on every request by default; workflows depending on per-request UA rotation must add `-evasion R` explicitly.

WAS THIS USEFUL? 👍 👎

◆ SAST / SCA / Code Security

Cloudsmith ⓘ changelog · Aug 1, 2026 CHANGELOG ↗

Cloudsmith is a cloud-native, universal package management platform that enables teams to securely host, manage, and distribute software artifacts across multiple formats.

Cloudsmith CLI 1.20.0 ships as a standalone binary, dropping the Python dependency, with a new bug bounty platform at `bounties.cloudsmith.com`.

- New one-line installer, refreshed Homebrew tap, and updated Docker image available for the standalone CLI.
- New bug bounty platform launched at `bounties.cloudsmith.com` for security researchers to submit vulnerability reports.

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Sublime Security ⓘ

Platform v1.87.25 (CrowdStrike Falcon Next-Gen SIEM and Fusion SOAR integrations) (202

BLOG ↗

Sublime Security is an AI-powered email security platform that detects and remediates advanced threats like phishing and business email compromise.

Sublime email events now stream into CrowdStrike Falcon Next-Gen SIEM, and Sublime Actions run natively in Falcon Fusion SOAR playbooks.

- Streams Sublime email security events (flagged message groups, user-reported messages) into CrowdStrike Falcon Next-Gen SIEM alongside endpoint, identity, and threat intelligence telemetry.
- Surfaces per-message triage context in Falcon Next-Gen SIEM: matched Sublime coverage, source IPs, URLs, attachment hashes, link-click activity, and ASA (Autonomous Security Analyst) verdict.
- Adds Sublime Actions as native steps in Falcon Fusion SOAR playbooks, enabling message investigation and enrichment, hunt result retrieval, Rule and List management, and remediation without leaving Falcon.
- Returns typed output from every Sublime Action in Fusion, allowing downstream playbook steps to branch on results without manual JSON parsing.

WAS THIS USEFUL? 👍 👎

Fastly ⓘ JavaScript SDK 3.44.0 (2026-07-27) BLOG ↗

Fastly is a cloud edge platform that accelerates, secures, and delivers websites, apps, and APIs by caching content closer to users globally.

Fastly JavaScript SDK 3.44.0 adds bot detection capability.

- Adds bot detection support to the Fastly JavaScript SDK.

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Runtime Security

NVIDIA OpenShell ⓘ v0.0.96 NOTES ↗

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

OpenShell v0.0.96 adds supervisor middleware content guard, Kubernetes PVC storage class config, policy-first OCI image identity, workspace authorization, and OTLP gateway tracing.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.0.96 https://github.com/NVIDIA/OpenShell.git
# already have the repo? check out this version:
$ git checkout v0.0.96
```

- Adds supervisor middleware content guard example for filtering or inspecting sandbox traffic at the supervisor layer.
- Supports configuring a custom `storageClassName` for workspace PVCs in Kubernetes deployments.
- Introduces policy-first OCI image identity resolution in the sandbox, giving security policies priority in image evaluation.
- Wires authorization checks into the workspace model, enabling access control enforcement at the workspace level.
- Exports gateway traces over OTLP, enabling distributed tracing observability for gateway activity.

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Huntress ⓘ Huntress API now supports creating IP-based rules for ITDR

NOTES ↗

Huntress is a managed threat detection and response platform that helps MSPs and enterprises detect and respond to security threats.

Huntress API gains an endpoint to create IP-based allow/block rules for Managed ITDR Unwanted Access.

› New API endpoint lets you programmatically create IP address-based rules for Managed ITDR Unwanted Access, accepting a single IP, a CIDR range, or a list of IPs in one call.

WAS THIS USEFUL? 👍 👎

Trend Vision One ⓘ

Service Gateway support for ECS clusters in Container Security (2026-07-30)

2 RELEASES · 2026-07-27 → 2026-07-30 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.

Trend Vision One Container Security now supports Service Gateway as a connection method for Amazon ECS clusters.

└──▷ HOW TO FIND IT

Route ECS cluster traffic through a Service Gateway instead of a direct internet connection — useful for air-gapped or private-network environments.

📍 In the console, go to Cloud Security → Container Security, open your Amazon ECS cluster connection settings, and select Service Gateway as the connection method.

› Supports Service Gateway as a connection method when configuring Amazon ECS cluster connections in Container Security.

▾ 1 more release in this issue · 2026-07-27 → 2026-07-30

Container Protection for Amazon ECS version 2.2.6 (2026-07-27) BLOG ↗

STABLE

Container Protection for Amazon ECS 2.2.6 adds Service Gateway forward proxy support and CodePipeline deployment updates.

› Supports using a Service Gateway as a forward proxy for Amazon ECS clusters.

› Supports CodePipeline standard deployment updates for OriginalTaskDefArn.

WAS THIS USEFUL? 👍 👎

◆ Detection Engineering

Datadog Stratus Red Team ⓘ v2.35.0 NOTES ↗ CODE ↗

Granular, Actionable Adversary Emulation for the Cloud

Adds new Azure attack technique to emulate AI Foundry API key exfiltration via local auth re-enablement.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.35.0 https://github.com/DataDog/stratus-red-team.git
# already have the repo? check out this version:
$ git checkout v2.35.0
```

└──▷ TRY IT

Emulate an attacker re-enabling local auth on an Azure AI Foundry account and exfiltrating its API keys — useful for validating detections on Azure Cognitive Services key-listing activity.

```
$ stratus detonate azure.persistence.exfiltrate-foundry-key
```

› New Azure technique `azure.persistence.exfiltrate-foundry-key` : re-enables local (key-based) authentication on an Azure AI Foundry (Cognitive Services) account and retrieves API keys via ListKeys, emulating a Persistence/Credential Access attack path.

└──▷ BREAKING ON UPGRADE

! The `azure.persistence.exfiltrate-foundry-key` technique requires the `ARM_SUBSCRIPTION_ID` environment variable (not `AZURE_SUBSCRIPTION_ID`) due to an upgrade to the azurerm Terraform provider 4.80.0.

WAS THIS USEFUL? 👍 👎

◆ Security Data Pipeline

Cribl ⓘ

What is your AI actually doing? Introducing the Cribl app for AI Observability (2026-0

BLOG ↗

Cribl is an observability pipeline platform that helps organizations collect, process, route, and transform machine data from any source to any destination.

Cribl launches AI Observability app — unified search, cost tracking, PII detection, and trace investigation across all AI models and providers.

└──▷ HOW TO FIND IT

Surface PII or credential leakage in AI sessions by reviewing Sensitive Data Traces — useful during a security review or incident triage.

📍 In Cribl.Cloud, open the AI Observability app › Security and Compliance Dashboard › Sensitive Data Traces, then filter by subcategory (PII, credentials, API keys) and by user or model to locate the exact trace or session where sensitive data appeared.

Track AI spend against budget targets to catch token overruns before they become a finance problem.

📍 In Cribl.Cloud, open the AI Observability app › Goals and Monitors, create a new monitor targeting month-to-date token spend, and set the budget threshold for your team or model.

Investigate a model quality regression by jumping from a dashboard anomaly directly into the full prompt and response payloads for that session.

📍 In Cribl.Cloud, open the AI Observability app › Sessions and Traces, filter the session list by model and time range, select the suspect session, and inspect the span timeline alongside full prompt, response, and tool-call payloads.

- New Cribl app for AI Observability provides a single platform to search, investigate, and report on AI telemetry across models, tools, and environments.
- Usage and Cost Dashboard surfaces spending trends, token consumption, top users and models, LLM efficiency anti-patterns, and an activity heatmap.
- Org View delivers a hierarchical roll-up of spend, tokens, and requests across the organization.
- Goals and Monitors continuously evaluate live AI telemetry against user-defined targets such as month-to-date token spend vs. budget.

- Security and Compliance Dashboard tracks sensitive data exposure rates, findings by type and user, tool-call audit trails, and content risk indicators.

+5 more

WAS THIS USEFUL? 👍 👎

◆ SIEM

Sumo Logic ⓘ

Apps, Solutions, and Collection Integrations - July Release (2026-07-31)

BLOG ↗

Sumo Logic is a cloud-native platform that collects, analyzes, and visualizes machine data and logs for security, observability, and operational intelligence.

Sumo Logic adds new dashboards, FERs, and monitors across 18+ apps, plus a new Terraform resource for Lambda invoke actions.

- Adds new and updated dashboards, field extraction rules (FERs), and monitors for Active Directory 2012+ (JSON), Artifactory 7, Azure Audit, ChatGPT Compliance, Cisco Meraki, Cloudflare Enterprise Audit - Cloud SIEM, Heroku, Host and Process Metrics, Host Metrics Linux, LiteLLM, Microsoft Office 365, Windows 2012+ (JSON), Windows 7+2008 (Legacy), Windows CSMA, Windows Performance, Zscaler Internet Access, and Zscaler Private Access.
- Migrates Azure Metrics collection from legacy ARM-based collection to the latest Azure Metrics Source.
- Adds new Terraform resource `sumologic_lambda_invoke_action` in SumoLogic Terraform Provider v3.2.9.

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

runZero

runZero 5.1.260731.2 (2026-07-31) BLOG ↗

runZero is a continuous asset intelligence platform that discovers, inventories, and monitors all connected devices and software across networks in real-time.

runZero 5.1 adds compliance-friendly AI workflows, autonomous discovery, enhanced integration framework, ITSM remediation handoffs, and improved Dragos OT enrichment.

- Adds compliance-friendly AI workflows for querying and surfacing asset data insights.
- Introduces autonomous discovery mode for automated, continuous attack surface intelligence.
- Enhanced integration framework with refined merge logic to accelerate custom integrations.
- Streamlined remediation handoffs available directly inside runZero or via ITSM integration.
- Improved Dragos integration enriches OT/ICS asset context and reduces data silos.

+1 more

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Secure Access (VPN / SASE / ZTNA)

DNSFilter ⓘ changelog · Aug 1, 2026 CHANGELOG ↗

DNSFilter is a cloud-based DNS security platform that blocks malicious websites, filters unwanted content, and protects networks from cyber threats in real time.

DNSFilter 3.6.10 adds DNS PreCheck v2, Brave SafeSearch enforcement, redesigned SafeSearch controls, and AppAware Sites filter.

└──▷ HOW TO FIND IT

Enable SafeSearch enforcement across all supported search engines at once inside a Filtering Policy.

> 📍 In the console, go to Filtering Policies › [select a policy] › Privacy tab › SafeSearch section, then click `Enforce All` to enable enforcement for Google, Bing, DuckDuckGo, Ecosia, Yandex, and Brave simultaneously.

Find unclassified domains in the Query Log to identify traffic that may need manual categorization or blocking.

> 📍 In the console, go to Query Log, open the filter panel, and select `Uncategorized` from the category filter to show only queries DNSFilter has not yet classified.

Scope AppAware reporting to a specific site in a mixed Core/Pro environment to audit per-site application usage.

> 📍 In the console, go to AppAware Reporting, open the filter bar, and select the desired site from the new Sites filter to view query data limited to that site.

- Introduces DNS PreCheck v2 for Windows Roaming Client, maintaining policy enforcement even on networks that hijack or redirect DNS traffic.
- Adds automatic tray process recovery so the system tray restarts itself if it stops unexpectedly, keeping status and controls available.
- Adds Sites filter to AppAware Reporting, giving Core plan and mixed Core/Pro environments query data scoped to specific sites.
- Supports SafeSearch enforcement on Brave browser in Filtering Policies, joining Google, Bing, DuckDuckGo, Ecosia, and Yandex.
- Redesigns the SafeSearch policy editor section with decoupled enforcement toggles and a new `Enforce All` shortcut to enable every SafeSearch engine at once.

+2 more

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

Auth0 ⓘ changelog · Aug 1, 2026 CHANGELOG ↗

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 adds AI agent identity, curated IP blocklists, org-scoped roles, cross-app access, and enterprise federation in a wave of new capabilities.

└──▷ TRY IT

Block all traffic from active TOR exit nodes and low-reputation IPs at the tenant level using curated Auth0 Threat Intel lists.

```
$ curl -X POST https://<tenant>.auth0.com/api/v2/network-acls \
  -H 'Authorization: Bearer <mgmt_api_token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "description": "Block TOR and low-reputation IPs",
    "active": true,
    "priority": 1,
    "rule": {
      "action": { "block": true },
      "match": {
        "auth0_managed": ["auth0.tor", "auth0.low_reputation"]
      },
      "scope": "authentication"
    }
  }'
```

Find a specific user or application across your tenant instantly without navigating menus.

> 📍 In the Auth0 Dashboard, press Cmd+K (or Ctrl+K), then type the user's email address or application name to search across Applications, APIs, Organizations, and Users in real time.

- Adds Global Search (Beta) to the Command Palette (Cmd+K), enabling real-time tenant-wide search across Applications, APIs, Organizations, and Users by name, ID, email, or identifier with one-click ID copying.
- Introduces Enterprise Connect (Beta), letting you federate existing SAML or OIDC authorization servers (including Okta) into Auth0 and layer on enterprise SSO, SCIM user provisioning, and self-service B2B onboarding with Actions-based claim enrichment and connection lifecycle events.

- Launches Curated Blocklists in Tenant ACLs (GA), integrating dynamically updated Auth0 Threat Intel categories — `auth0.low_reputation`, `auth0.tor`, `auth0.proxy`, `auth0.vpn`, `auth0.icloud_relay_proxy` — into Network ACL rules via the `auth0_managed` matcher block in the Management API.
- Introduces Agents as Principal (Early Access), giving AI agents a unique first-class identity with their own credentials, audit trail, and delegation chain encoding in tokens — separate from human users and shared clients.
- Adds Token Vault Privileged Worker (Early Access), allowing background agents to authenticate via Private Key JWT or mTLS and retrieve a specific user's third-party tokens (Gmail, Drive, Slack, etc.) from Token Vault without an active user session, with per-connection and per-scope credential pinning.

+5 more

WAS THIS USEFUL? 👍 👎

Didit ⓘ snapshot-20260801 NOTES ↗

Didit is a decentralized identity verification platform enabling secure digital identity management and verification for users and applications.

Didit adds Travel Rule compliance, Console Copilot, Test mode sandbox, device integrity attestation, and expanded KYB/AML capabilities.

└──▷ HOW TO FIND IT

Enable ongoing AML monitoring for a specific user directly from the Users table without navigating away.

> 📍 In the Console, go to Users › find the user row › toggle the Monitoring column switch › review the cost estimate › confirm to enable monitoring.

Use the modular Flutter SDK variant to include only core verification without NFC or autodetection, reducing native footprint.

```yaml
dependencies:
  didit_sdk_core: ^4.5.3
```

- Adds end-to-end Travel Rule compliance: encrypted IVMS 101 sender/recipient exchange, TRP messaging, secure email fallback, VASP directory, self-custody wallet ownership proof, and preset EU Transfer of Funds Regulation rules.
- Introduces Didit Copilot in the Business Console — a resizable AI panel that builds workflows, applies filters, and navigates dialogs via natural language, voice input, or file attachment, with explicit confirmation gates for writes/deletes.
- New applicant ID Verification Data Review step lets users confirm or correct extracted document fields before submission, with configurable outcomes by mismatch severity, MRZ-protected fields, and full correction history in session details.
- Adds complete Test mode for sandbox applications: choose approved/declined/in-review scenarios, upload sample documents, enter any OTP, and assert the armed scenario via `sandbox_scenario` in the v3 decision payload — no external providers contacted.
- New Device & Capture Integrity signals: Apple App Attest and Google Play Integrity attestation, frame injection detection with attack subtype reporting, virtual-camera risk flagging, and per-workflow policy actions (decline/review/record).

+5 more

WAS THIS USEFUL? 👍 👎

Clerk ⓘ Self-serve SSO for OIDC (2026-07-31) BLOG ↗

Clerk is a user authentication and identity management platform that provides developers with pre-built UI components, APIs, and SDKs for sign-up, sign-in, and user management.

Clerk lets end-customer IT admins self-configure OIDC SSO connections directly from the OrganizationProfile UI.

└──▷ HOW TO FIND IT

Surface the Security tab to your customers' IT admins so they can set up their own OIDC SSO without involving your support team.

> 📍 In your app, render <OrganizationProfile /> and direct IT admins to the Security tab to configure their OpenID Connect connection.

› Enables organization IT admins to configure their own OpenID Connect SSO connections self-serve via the Security tab in <OrganizationProfile />.

WAS THIS USEFUL? 👍 👎

◆ Data Security & DLP

Varonis

changelog · Aug 1, 2026

CHANGELOG ↗

Varonis is a data security platform that detects and stops insider threats, data breaches, and ransomware attacks across cloud and on-premises environments.

Varonis adds Search & Export APIs, IP-based tenant lockdown, VAST multi-tenant visibility, and expanded AI agent governance in Atlas.

- New Search API provides programmatic access to Varonis data — events, identities, resources, permissions, memberships, and alerted events — to support investigations, workflow automation, and SIEM/SOAR integrations.
- Label lifecycle controls let administrators automatically remove or preserve Varonis-applied Microsoft Purview labels when the triggering conditions no longer apply.
- Automatic label downgrade prevention compares existing Microsoft Purview labels against Varonis recommendations and only applies changes that result in stronger protection.
- Segment information can now be included in Syslog messages, event publishing workflows, and MDDR escalation emails to improve alert routing and downstream correlation.
- AI Investigation Sessions gain an Intent Timeline offering a chronological view of user intent, agent behavior, and tool activity within a session.

+2 more

WAS THIS USEFUL? 👍 👎

Immuta ⓘ snapshot-20260801 NOTES ↗

Immuta is a data security platform that automates access control, privacy policy enforcement, and compliance monitoring across cloud data environments.

Immuta adds richer Connections controls, split request forms for data products, Redshift viewless data discovery, and new managed identity groups.

└──▷ HOW TO FIND IT

Force-delete a stuck UNHEALTHY Snowflake or Unity Catalog connection without waiting for it to recover.

📍 In the Immuta console, navigate to Connections, locate the connection showing UNHEALTHY status, open its detail page, and select Force Delete.

- Adds integration health states (ACTIVE, INACTIVE, UNHEALTHY) and per-connection settings directly within Connections for Databricks Unity Catalog and Snowflake.
- Introduces per-object policy sync toggle to control whether Immuta pushes policies down to a given data object, with visibility into child object configuration and a Custom label when child settings differ from the parent.
- Adds individual detail pages for leaf data objects, including a direct link to the corresponding data source.
- Enables bulk or individual tag assignment and removal at the database or schema level, with tag inheritance flowing to all attached data sources.
- Makes the behavior of the New tag configurable in App Settings (default: enabled for columns, disabled for data sources).

+7 more

└──▷ BREAKING ON UPGRADE

- ! Immuta policy role names used to grant users access to Snowflake data sources will be renamed as part of the Snowflake integration architecture update rolling out beginning July 23, 2026; existing policy roles will be recreated under new names.
- ! Integration error banners for Snowflake validation failures will no longer be displayed; error details are now available only through the new Connections experience.
- ! When a data source is disabled, Immuta now revokes data owners' Immuta-managed grants in the data platform (behavior change release, on by default 8/1).

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

CISO Assistant ⓘ v3.20.5 NOTES ↗

CISO Assistant is a one-stop-shop GRC platform for Risk Management, AppSec, Compliance & Audit, TPRM, BIA, Privacy, and Reporting. It supports 150+ 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 v3.20.5 adds LPM/OIV metrics definitions, cybersecurity metrics translations, and expanded evidence file previews.

└──▷ GET THIS VERSION

```
$ git clone --branch v3.20.5 https://github.com/intuitem/ciso-assistant-community.git
# already have the repo? check out this version:
$ git checkout v3.20.5
```

- Adds 10 LPM/OIV required metrics definitions to the library, supporting regulated French operators of vital importance.
- Adds translations for core cybersecurity metrics.
- Expands in-platform preview support to additional evidence file types.

└──▷ BREAKING ON UPGRADE

! Old invalid Implementation Groups are pruned when updating a framework — existing mappings to invalid groups will be removed on framework update.

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Kiro ⓘ Tangent Side-Conversations and Per-Tool Token Breakdown NOTES ↗

Kiro is an AI-powered IDE by AWS that uses "specs" to translate requirements into structured plans, then automatically generates and implements code.

Kiro gains `/tangent` side-conversations and per-tool token breakdown in `/context`.

└──▷ TRY IT

Quickly look something up mid-task in an isolated branch, then return to your main workflow without cluttering the primary thread.

```
$ kiro-cli --v3
# inside the session:
/tangent research-auth
# ... explore freely ...
/tangent root
```

- New `/tangent` command lets you branch into named side-conversations that inherit full conversation history, then return to the main thread without polluting it.
- Browse your entire conversation tree with `/tangent ls` and jump to the root from any depth with `/tangent root`.
- The `/context` command now shows a per-tool token breakdown so you can see exactly what is consuming your context window.

WAS THIS USEFUL? 👍 👎

Cline ⓘ sdk/sdk/v0.0.68 NOTES ↗ CODE ↗

Autonomous coding agent as an SDK, IDE extension, or CLI assistant.

Cline SDK v0.0.68 adds display-ready model names, ClinePass provider, UTF-8 PowerShell stdin, and Organization selector for ACP.

└──▷ GET THIS VERSION

```
$ git clone --branch sdk/sdk/v0.0.68
https://github.com/cline/cline.git
# already have the repo? check out this version:
$ git checkout sdk/sdk/v0.0.68
```

- Adds `fetchClineRecommendedModels` returning display-ready model names resolved through the model catalog (including Vercel and OpenRouter id aliases) under a shared timeout budget, so hosts no longer need to map ids to names themselves.
- Adds Organization selector to ACP, letting users switch between personal account and org contexts without leaving the session.
- Adds ClinePass as a selectable provider on ACP (id: `cline-pass`, Sign in with ClinePass).
- On Windows, PowerShell commands now travel over UTF-8 stdin via getShellInvocation(), eliminating truncation from Windows command-line length limits and corruption of non-ASCII characters caused by active code page mismatches.
- Exports finish-reason and auth-error helpers (`describeAgentError` and friends) for use by SDK consumers describing agent errors.

+1 more

└──▷ BREAKING ON UPGRADE

! getShellArgs() is now deprecated and replaced by getShellInvocation(); callers relying on the old function should migrate to getShellInvocation().

WAS THIS USEFUL? 👍 👎

Crush ⓘ v0.88.0 NOTES ↗ CODE ↗

Glamourous agentic coding for all

Crush v0.88.0 adds `.crushrc` bash-based config, `permissions deny`, AWS Bedrock SSO re-auth, and new crushrc builtins for providers, models, MCPs, LSPs, and hooks.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.88.0
https://github.com/charmbracelet/crush.git
# already have the repo? check out this version:
$ git checkout v0.88.0
```

└──▷ TRY IT

Bootstrap a dotfiles-friendly crushrc that adds a local Ollama provider, auto-approves safe tools, and loads machine-specific overrides that stay out of git.

```
$ cat ~/.config/crush/crush.sh
# Add Ollama.
provider add ollama --type ollama --base-url
"http://localhost:11434/v1"

# Register a model on Ollama.
model add ollama/llama3.3 --name "Llama 3.3" --context-window 128000

# Auto-approve read/write tools.
permissions allow view edit

# Load machine-specific secrets (kept in .gitignore).
source "$XDG_CONFIG_HOME/local-overrides.sh"
```

Apply different skill paths per hostname using crushrc conditionals and `option reset`.

```
$ cat >> ~/.config/crush/crush.sh <<'EOF'
if [[ $HOSTNAME == "workstation" ]]; then
    option skill-path "$HOME/work-skills"
else
    option reset skill-path
fi
EOF
```

- Adds `.crushrc` bash-based configuration file, replacing JSON config with a scriptable shell format that supports conditionals, `source` includes, and environment variable expansion.
- Adds `permissions deny` command in crushrc to explicitly hide specific tools from the agent.
- Adds `permissions allow` command in crushrc to auto-approve tools without prompting.
- Adds `provider add` and `model add` crushrc builtins for registering custom providers and models (e.g. local Ollama instances).
- Adds `mcp add` / `mcp remove` crushrc builtins for managing MCP servers directly from the shell config.

+7 more

WAS THIS USEFUL?  

DEPLOY

◆ Agentic Infrastructure

emisar ⓘ v0.36.0 3 RELEASES · 2026-07-31 NOTES ↗ LATEST STABLE

An MCP that lets AI tools securely connect to your infrastructure, write IaaS code, debug issues, and assist during incidents - without risking production stability. Built for security teams to approve and infrastructure teams to experience like magic.

Emisar v0.36.0 adds staged runbooks with typed inputs and parallel execution, MCP 2026-07-28 routing, and 91 action packs with bounded diagnostics.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.36.0
https://github.com/AndrewDryga/emisar.git
# already have the repo? check out this version:
$ git checkout v0.36.0
```

- Adds staged runbooks with typed inputs, sequential or parallel stage execution against selected runner groups, named step outputs, success condition testing, and explicit wait bounds.
- Adds a single pre-execution approval gate that freezes the complete runbook execution plan before work begins.
- Adds canonical JSON runbook definition format shared across the console, MCP, and execution pages, with attempt, output, wait, and terminal cause history.
- Adds OIDC discovery and JWKS refresh under a shared bounded address policy that rechecks the actual response received; changing an issuer clears credentials tied to the old one.
- Adds atomic SCIM group patch application in wire order, with body bounding before authentication and automatic session and identity link retirement when a connection is disabled.

+4 more

└──▷ BREAKING ON UPGRADE

! Disabling a SCIM connection now retires the sessions and pending identity links it vouched for — active sessions tied to a disabled SCIM connection will be terminated on upgrade.

! Pack actions now fail on missing source commands and HTTP error responses rather than returning an empty success — any automation that depended on silent empty-success behavior will begin receiving failures.

▾ **2 more releases in this issue** · 2026-07-31

`mcp-v0.5.0` **NOTES ↗** **STABLE**

emisar mcp-v0.5.0 expands its infrastructure diagnostics catalog.

└──▷ GET THIS VERSION

```
$ git clone --branch mcp-v0.5.0
https://github.com/AndrewDryga/emisar.git
# already have the repo? check out this version:
$ git checkout mcp-v0.5.0
```

› Expands the infrastructure diagnostics catalog with additional checks.

`runner-v0.16.0` **NOTES ↗** **STABLE**

emisar runner v0.16.0 expands its infrastructure diagnostics catalog.

└──▷ GET THIS VERSION

```
$ git clone --branch runner-v0.16.0
https://github.com/AndrewDryga/emisar.git
# already have the repo? check out this version:
$ git checkout runner-v0.16.0
```

› Expands the infrastructure diagnostics catalog with additional checks.

WAS THIS USEFUL? 👍 👎

◆ Local LLM Runtimes

vMLX ⓘ v1.6.19 NOTES ↗

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

vMLX 1.6.19 adds native-MTP diagnostics, model-owned sampling defaults, separate macOS Tahoe builds, and scoped sparse-cache blocks for MiniMax M3.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.6.19 https://github.com/jjang-ai/vmlx.git
# already have the repo? check out this version:
$ git checkout v1.6.19
```

- Adds native-MTP health and profiling telemetry exposing bounded cache-lifecycle, acceptance, and phase-timing metrics for Qwen MTP models.
- Introduces model-owned generation defaults: temperature, Top P, Top K, repetition penalty, and output limits now hydrate from the selected model bundle in new and restored chats.
- Ollama requests now preserve an explicitly supplied `top_k` value, including `0`, through request translation.
- Automatic prompt limits are now derived from the actually loaded model's configuration, bounded by its declared context ceiling and current memory budget.
- MiniMax M3 native sparse-cache blocks are scoped to the prompt-prefill shape, preventing numerically incorrect Lightning Indexer state restoration across mismatched prefill shapes.

+7 more

WAS THIS USEFUL? 👍 👎

OTHER / UNCATEGORIZED

◆ UNCATEGORIZED

OpenOSINT ⓘ v2.25.0 NOTES ↗

AI-powered OSINT agent with interactive REPL, MCP server, and CLI. 19 tools.

OpenOSINT v2.25.0 adds global HTTP/SOCKS5 upstream-proxy support and cloud billing OAuth for web-facing tools.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.25.0
https://github.com/OpenOSINT/OpenOSINT.git
# already have the repo? check out this version:
$ git checkout v2.25.0
```

- Adds global upstream-proxy support (HTTP and SOCKS5) for all web-facing tools.
- Introduces cloud billing OAuth integration and associated tooling.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · August 1, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe