THE CYBER TOOLCHAIN

NO. 121

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED OCTOBER 26, 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 45 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 13 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. Plerion can now answer "where is this package, in this version range" across every asset, which is the question new CVE forces; JumpCloud began streaming directory events to

vim ? help

SIEM in OCSF and blocked local agent uninstalls; Lumia pulled Claude Enterprise conversations, uploads and agent activity into view.

> IDENTIFY
>
> **Answer "am I running that package" without a one-off SBOM hunt**
>
> Plerion's Find by package search returns every asset running a given package within a version range, with deep links into each SBOM tab — the lookup teams otherwise do by hand or by script each time a CVE lands. OpenQodex extends its code graph to Java, so call chains in review output come from the graph rather than a build.
>
> Plerion · OpenQodex

> DETECT
>
> **Get directory events into the SIEM, and see what staff are doing inside Claude**
>
> JumpCloud's OCSF/RAW export means identity activity lands in a normalized schema instead of needing a custom parser per tenant, and Agent Uninstall Protection removes the quiet gap where a local admin kills the agent before anything is logged. Lumia's Claude Compliance API integration surfaces Enterprise conversations, file uploads and agent activity, with optional inline enforcement — the first visibility most teams have into a sanctioned LLM they otherwise treat as a black box.
>
> JumpCloud · Lumia

> PROTECT
>
> **Push attack-surface findings straight into a scan, and keep tail latency honest on the AI gateway**
>
> Veracode's EASM now scores discovered exposure by actual vulnerability and exports directly into DAST Essentials, closing the usual manual handoff between "we found this host" and "someone scanned it." Lakera's request latency percentiles chart shows the tail, not the average — the part that determines whether an inline guardrail gets ripped out of the request path.
>
> Veracode · Lakera

APPLICATION SECURITY

◆ Web Application Security

caido

Feedback ⓘ v0.59.0 NOTES ↗ RANK

Caido releases, wiki and roadmap

> Caido v0.59.0 introduces AI-generated workflows via AWS Bedrock and OpenAI, adds cURL import in Replay, extends Traffic Control with TLS pass-through and in-scope-only logging, and lets the desktop app connect to multiple instances at once.

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

01 **cURL import in Replay** NEW 65

Replay now supports creating requests directly from copied cURL commands via a Create from cURL option, letting practitioners recreate requests from other tools without manually rebuilding them.

Quickly recreate a request observed in another tool without manually rebuilding it in Caido.

📍 In Replay, select Create from cURL, paste your cURL command, and send.

— Exact UI path and workflow provided v0.59.0

02 **TLS pass-through and scoped logging in Traffic Control** NEW 65

Traffic Control gains TLS pass-through, enabling raw TLS traffic to bypass interception, and a 'log only in-scope requests' option that suppresses out-of-scope traffic from the recorded request log to reduce noise.

Reduce log volume during a scoped engagement by recording only traffic that matches your defined scope.

📍 In Traffic Control settings, enable Log only in-scope requests to suppress out-of-scope traffic from the request log.

— Named settings with one exact usage step v0.59.0

THINNER COVERAGE BELOW

03 **AI-generated workflows from prompts** NEW 50

Caido can now generate workflows from natural-language prompts, with support for AWS Bedrock and an OpenAI OAuth flow for personal subscriptions.

– Names providers but no setup steps given v0.59.0

04 **Multi-instance connections in desktop app** NEW 25

The Desktop app now supports simultaneous connections to multiple Caido instances.

– One-line description with no mechanism or steps v0.59.0

WAS THIS USEFUL? 👍 👎

PortSwigger Burp Suite Feedback ⓘ

Professional / Community 2026.10.1 (2026-10-26) BLOG ↗ RANK

Burp suite is a we enable the world to secure the web. Burp Suite, the Web Security Academy, and world-leading research from PortSwigger â the AppSec communityâs home.

> Burp Suite 2026.10.1 expands integration between manual testing tools and Burp AT, making it easier to feed evidence from more parts of the suite into AT tasks.

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

01 **Send requests/responses to Burp AT from more tools** IMPROVED 35

Burp Suite now lets you send requests and responses to Burp AT from more Burp tools, making it easier to bring manual testing evidence into a task.

– Names the capability but not which tools or how to trigger it

Professional / Community 2026.10.1 (202…

WAS THIS USEFUL? 👍 👎

◆ SAST / SCA / Code Security

opentaint

Feedback ⓘ analyzer/2026.10.26.c624add NOTES ↗ RANK

The open source taint analysis engine for the AI era. A formal dataflow analysis tool you can customize and self-host, built so AI agents drive your application security analysis without burning tokens on every scan.

> OpenTaint's analyzer release adds a new wildcard operator for writing taint rules and tightens the precision of passthrough models.

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

01 **Star operator for taint rules** NEW 45

The analyzer adds the `$*` star operator for use in taint rules (#340), giving rule authors a new wildcard construct when defining dataflow taint patterns.

— Names the exact operator but not its syntax or semantics analyzer/2026.10.26.c624add

02 **More precise passthrough models** IMPROVED 25

Passthrough models used in taint tracking are made more precise (#315), improving how the analyzer propagates taint through functions that pass values through.

— States the change but not the mechanism or scope analyzer/2026.10.26.c624add

WAS THIS USEFUL? 👍 👎

OpenQodex

Feedback ⓘ openqodex@0.15.0 NOTES ↗ RANK

Open source code review that runs in your coding agent before you push. Scanners plus a separate AI reviewer, on your own login, no key.

> OpenQodex 0.15.0 extends its code graph with Java support, enabling call-chain analysis in review output without requiring a build step.

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

01 **Java support in the code graph** NEW 57

The code graph now parses Java, reading types, methods, constructors, imports, static imports, and calls with no build step required. Review output names callers of changed Java code, each annotated with its tier.

— Names mechanism and elements parsed but no config or command shown openqodex@0.15.0

WAS THIS USEFUL? 👍 👎

Veracode

Feedback ⓘ EASM updates (2026-10-26) BLOG ↗ RANK

Veracode is a cloud-based application security platform that scans code, binaries, and running applications to find and help remediate software vulnerabilities.

> Veracode's EASM module gained vulnerability-aware risk scoring, built-in GDPR/NIS2/DORA compliance evidence collection, a redesigned interface with multi-project and scheduling controls, and a direct export path into DAST Essentials.

└──▷ **WHAT SHIPPED · 8 FEATURES** most completely described first ? what's the number?

01 **Export EASM assets to DAST Essentials** NEW 58

Enables exporting web applications from EASM directly into DAST Essentials by marking assets as DAST Candidates.

– Names exact flag (DAST Candidates) and target product EASM updates (2026-10-26)

02 **Compliance evidence collection for GDPR, NIS2, DORA** NEW 52

EASM collects compliance evidence including cookie consent tracking, third-party data flows, destination countries, and privacy, legal, and copyright documentation to support GDPR, NIS2, and DORA assessments.

– Names evidence types but no navigation or export detail EASM updates (2026-10-26)

03 **Vulnerability-aware EASM risk scoring** IMPROVED 48

EASM now validates components against the EASM knowledge base so risk scores reflect real vulnerabilities present in a given software version, rather than scoring based solely on software age.

– Explains mechanism but no concrete config or metric given EASM updates (2026-10-26)

04 **Redesigned EASM interface with Legacy UI option** IMPROVED 45

Adds a redesigned EASM interface with improved navigation; the previous interface remains accessible as `Legacy UI`.

– Names Legacy UI toggle but no further mechanism EASM updates (2026-10-26)

05 **Findings view with prioritization and reporting** NEW 45

Adds a Findings view with improved prioritization workflows and expanded reporting capabilities.

— Names a UI area as clear starting point, thin on mechanism EASM updates (2026-10-26)

06 **Multi-project visibility, scheduling, and AI-powered intelligence**

NEW 38

Introduces multi-project visibility, scan scheduling, and AI-powered intelligence for centralized risk management and scan orchestration across EASM.

— Lists capabilities without specifics on how they work EASM updates (2026-10-26)

07 **Real-time scan status notifications** NEW 30

Delivers real-time in-app notifications when scans complete, fail, or are cancelled.

— Bare description, no settings or triggers detailed EASM updates (2026-10-26)

08 **Issues capability for remediation focus** NEW 28

Adds an Issues capability to streamline remediation efforts and improve focus on cyber hygiene.

— Very thin, no mechanism or navigation detail EASM updates (2026-10-26)

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

Mobile Verification Toolkit

Feedback ⓘ v2026.10.26

NOTES ↗ CODE ↗ RANK

MVT (Mobile Verification Toolkit) helps with conducting forensics of mobile devices in order to find signs of a potential compromise.

> MVT added support for Python 3.15, extending its supported runtime range.

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

01 **Python 3.15 support** IMPROVED 40

MVT now runs on Python 3.15, extending the supported runtime range alongside existing support for Python 3.10–3.14.

— Names exact Python versions but no further mechanism detail v2026.10.26

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Cloud Security Posture

Plexicus

Feedback ⓘ

Plexicus v1.2.42: Next-Gen AI Pentest Engine, Live Pentest War Room & Automations That S

NOTES ↗ RANK

Plexicus validates security findings with evidence and helps your team fix what matters. AI Swarm Pentest, Deep Code Analysis, Remediation and XBOM.

> Plexicus upgraded its AI Pentest engine and wizard, added a live Pentest War Room and PlexiFlow automation testing, and in v1.2.71 replaced the connector catalog with a Scan Modules settings page alongside a new role permission matrix and compliance and security hardening work.

└──▷ **WHAT SHIPPED · 9 FEATURES** most completely described first ? what's the number?

01 Scan Modules settings page replaces connector catalog

75

BREAKING

The old connector catalog is replaced by a new Scan Modules settings page for managing scan integrations. In the Plexicus UI, go to Settings > Scan Modules to enable or disable individual scan modules for your tenant; any bookmarks or documented paths to the old connector catalog no longer apply after upgrading.

After upgrading, configure which scan modules are active for your tenant in place of the old connector catalog.

> 📍 In the Plexicus UI, go to Settings › Scan Modules, then enable or disable individual scan modules for your tenant.

— Exact UI path and explicit migration/breaking note given.

Plexicus v1.2.71: Scan Modules, Role Ma…

02 View/Edit/Manage role permission matrix NEW

75

Introduces a full View/Edit/Manage role permission matrix for granular access control across the platform. In the Plexicus UI, go to Settings > Roles, select a role, and use the matrix to set per-capability access.

Assign fine-grained View/Edit/Manage permissions to a role to enforce least-privilege access across teams.

> 📍 In the Plexicus UI, go to Settings › Roles, select a role, and use the View / Edit / Manage permission matrix to set per-capability access.

– Exact UI navigation and permission levels named.

Plexicus v1.2.71: Scan Modules, Role Ma…

THINNER COVERAGE BELOW

03 **AI Pentest engine upgrade and wizard rework** IMPROVED

45

Upgrades the AI Pentest feature to a next-generation scanning engine, then reworks the AI Pentest Wizard with an updated guided experience for penetration testing workflows.

– No mechanism or UI path given for either change.

Plexicus v1.2.43: AI Pentest Wizard Rew… Plexicus v1.2.42: Next-Gen AI Pentest E…

04 **Security hardening pass** IMPROVED

40

Delivers a comprehensive security hardening pass covering tenant boundary isolation, exports, and authentication.

– Names scope areas but no specific fixes or mechanisms.

Plexicus v1.2.71: Scan Modules, Role Ma…

05 **PlexiFlow per-node automation testing** NEW

35

Introduces per-node automation testing with data mapping via PlexiFlow.

– Names PlexiFlow but no config or usage steps given.

Plexicus v1.2.43: AI Pentest Wizard Rew…

06 **Live Pentest War Room with live board** NEW

30

Adds a live Pentest War Room for real-time collaboration during active pentests, later extended with a live War-Room board.

– No detail on what the board shows or how collaboration works.

Plexicus v1.2.43: AI Pentest Wizard Rew… Plexicus v1.2.42: Next-Gen AI Pentest E…

07 **Repo-centric asset views** NEW

30

Adds repo-centric asset views for browsing findings and assets organized by repository.

– No navigation path or filter options given. Plexicus v1.2.43: AI Pentest Wizard Rew…

08 **Richer certification question types and lifecycle** NEW

25

Adds richer question types and lifecycle management to certifications.

– Thin description, no question types or lifecycle stages named.

Plexicus v1.2.42: Next-Gen AI Pentest E…

09 **Unified compliance controls** IMPROVED

25

Unifies compliance controls into a single location for centralized policy management.

— No location path or control list given. Plexicus v1.2.71: Scan Modules, Role Ma…

└──▷ **BREAKING ON UPGRADE**

! The old connector catalog is replaced by the new Scan Modules settings page — any bookmarks or documented paths to the connector catalog will no longer apply.

WAS THIS USEFUL? 👍 👎

◆ **CNAPP**

Plerion

Feedback ⓘ Find every asset that runs a package: NOTES ↗

RANK

Plerion is a cloud security platform that detects misconfigurations, vulnerabilities, and threats across cloud environments and provides remediation guidance.

> Plerion added a Find by package search on the Assets page, letting teams locate every asset running a given package within a version range, complete with SBOM tab deep links.

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

01 **Find by package search on Assets page** NEW 80

A new Find by package search on the Assets page locates every asset running a given package, supporting version range filtering (e.g. `>= 2.0, < 2.15.0`) and returning exact version, environment, owner, and exposure per asset. Every package listed on an asset's SBOM tab now links directly to the Find by package view for that package.

When a package release is reported as compromised, quickly find every asset in your inventory running a vulnerable version range.

> 📍 In the Plerion platform, go to Assets › Find by package, enter the compromised package name (or paste a list), then enter a version range such as `>= 2.0, < 2.15.0` to see each affected asset with its exact version, environment, owner, and exposure.

— Names exact UI path, filter syntax, and returned fields.

Find every asset that runs a package:

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

syzkaller

Feedback ⓘ changes since 2026-10-23 CODE ↗

syzkaller is an unsupervised coverage-guided kernel fuzzer

syzkaller adds AI root cause analysis in bug reports and GCE image auto-deletion with reuse for unchanged local images.

Adds `auto_delete` GCE image lifecycle management via the `gce.LabelAutoDelete` and `gce.LabelLastActive` labels, enabling external jobs (e.g., an Argo CronWorkflow in syz-cluster) to delete stale images older than `gce.StaleImageAge`; requires `gce_image` to be empty in the VM config.

Reuses an existing GCE image when the local image file is unchanged, avoiding redundant image uploads.

Includes AI-generated root cause analysis summaries in dashboard bug report emails.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

JumpCloud

Feedback ⓘ Release Notes 2026 (2026-10-26) BLOG ↗

RANK

JumpCloud makes it simple to manage Windows, Apple, Linux, and Android devices and to deliver secure access with SSO, MFA, Zero Trust, RADIUS, and more.

> JumpCloud's 2026 release adds SIEM integration with OCSF/RAW export formats and Agent Uninstall Protection as the headline security additions, alongside new REST APIs for AI agent management, an MCP Server for Users, custom risk policies, and several User Portal and Apple MDM enhancements.

└──▷ **WHAT SHIPPED · 10 FEATURES** most completely described first ? what's the number?

01 **Agent Uninstall Protection** NEW 93

Adds Agent Uninstall Protection, enabled by default for all devices running JumpCloud agent v2.179.2 or later on macOS, Windows, and Linux, requiring a per-device maintenance token to uninstall; tokens rotate 60 minutes after being viewed and Directory Insights logs failed uninstall attempts, successful uninstalls, and exemption policy changes. A Disable Agent Uninstall Protection policy can exempt specific devices during maintenance, troubleshooting, or imaging.

Exempt a specific device from Agent Uninstall Protection during imaging without disrupting protection on the rest of the fleet.

📍 In the Admin Portal, go to Device Management › Devices › Settings › Agent Uninstall Protection and assign the Disable Agent Uninstall Protection policy for macOS, Windows, or Linux to the target device or device group.

— Version number, token rotation time, policy name and UI path all given.

Release Notes 2026 (2026-10-26)

02 **MCP Server for Users** NEW 83

Adds JumpCloud MCP Server for Users, enabling OAuth-based connections from AI clients to User Portal capabilities; admins enable it at `Settings > JumpCloud AI` and can configure automatic session expiration or revoke sessions manually.

Enable the JumpCloud MCP Server for Users so staff can perform User Portal tasks from their AI clients without leaving their tooling.

📍 In the Admin Portal, go to Settings › JumpCloud AI and toggle on MCP Server for Users. Optionally configure an automatic session expiration window. Users can

then view and revoke their own sessions at Security › JumpCloud MCP in the User Portal.

— Exact enable/revoke steps given via usage example. Release Notes 2026 (2026-10-26)

03 **SIEM integration in Directory Insights** NEW 80

Adds SIEM Integration in Directory Insights supporting continuous API pull ingestion using an existing API key in `RAW` or `OCSF -normalized` formats, plus asynchronous historical export jobs for up to 7-day windows across a 13-month retention lookback delivered as JSON or CSV files with email notification.

— Formats and windows named, but no exact API endpoint given.

Release Notes 2026 (2026-10-26)

04 **Custom Messaging in User Portal** NEW 75

Adds Custom Messaging feature in User Portal (`Settings > User Portal > Custom Messaging`) to create login dialogs and announcement banners scoped by user group with configurable severity/message type.

— Exact UI path named, mechanism described. Release Notes 2026 (2026-10-26)

05 **Agents and Agent Groups management APIs** NEW 73

Adds REST APIs for AI Agent and Agent Group management — Agents API and Agent Groups API — enabling programmatic registration, credential management, group membership, and application assignment.

— API names given but no exact endpoint paths or methods. Release Notes 2026 (2026-10-26)

06 **User Portal Asset Visibility and Acknowledgement** NEW 72

Adds User Portal Asset Visibility and Acknowledgement under `Device Management > Asset Management > Settings and Fields > General Settings`, giving users visibility into assigned assets and letting admins request acknowledgement recorded in Asset History.

— Exact settings path and recorded outcome named. Release Notes 2026 (2026-10-26)

07 **Custom Risk Policies for access risk** NEW 68

Adds Custom Risk Policies (Access Risk) to tailor risk detection for Admin Portal, User Portal, device, and SSO application logins by user group or application, with configurable risk factors, score contributions, and policy precedence.

— Scope and configurability described but no exact UI path.

Release Notes 2026 (2026-10-26)

08 **App Settings Privacy policies for Apple MDM** NEW 68

Adds two Apple MDM privacy policies: `User Level macOS App Settings Privacy` (macOS 27+, supervised Macs, supports Accessibility, Bluetooth, Camera, Dictation, Local network, Location, Microphone) and `Device Level iOS and iPadOS App Settings Privacy` (iOS/iPadOS 27+, supports Bluetooth, Camera, Dictation, Local Network, Location, Location Accuracy, Microphone).

— Policy names and supported categories named, no UI path given.

Release Notes 2026 (2026-10-26)

THINNER COVERAGE BELOW

09 **User Portal Folders** NEW 45

Adds User Portal Folders so end users can organize assigned applications into private personal folders on the All Applications page.

— Names the exact page but little mechanism beyond that. Release Notes 2026 (2026-10-26)

10 **Custom Banned Password List** NEW 35

Adds Custom Banned Password List to Password Policies, allowing admins to block specific words, terms, and phrases from user passwords.

— Bare description with no location or limits given. Release Notes 2026 (2026-10-26)

└──▷ ALSO FROM THESE RELEASES

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI Runtime Defense & Guardrails

Lakera

Feedback ⓘ snapshot-20261026 NOTES ↗ RANK

Lakera is an AI security platform that protects large language model applications from prompt injection, data leakage, and harmful content through real-time guardrails and APIs.

> Lakera's Analytics page now includes a request latency percentiles chart for Guard API traffic, giving teams visibility into tail-latency behaviour over time.

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

01 Request latency percentiles chart in Analytics NEW

65

The Analytics page adds a chart plotting `p25`, `p50` (median), `p75`, and `p95` latency of Guard API requests over time, with hover-to-inspect tooltips and per-percentile show/hide controls via the legend.

Identify tail-latency regressions in your Guard API traffic after a deployment or traffic spike.

> 📍 In the Lakera dashboard, go to Analytics › Request Latency Percentiles chart. Hover over a time bucket to read p25/p50/p75/p95 values, then click a legend entry (e.g. `p95`) to isolate that percentile and confirm whether tail latency exceeds your SLO threshold.

— Names exact percentiles and UI controls but no thresholds or limits. snapshot-20261026

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ Pentest Distributions

OffSec Kali Linux

Feedback ⓘ

Kali Linux 2026.3 Release (Build-Scripts Refresh) (2026-10-26) BLOG ↗ RANK

Home of Kali Linux, an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments.

> Kali Linux 2026.3 refreshes the build-scripts with container-based builds and new customization flags, adds six new tools to the network repositories, bumps the kernel to 7.1.5, updates KDE Plasma to 6.7, and significantly expands NetHunter with WearHunter, NFC Arsenal, KernelSU support, TicWatch wardriving, and nine new device kernels.

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

01 Containerized builds and build-time flags for build-scripts

NEW 85

Each refreshed build-script now includes `build-in-container.sh`, which auto-detects Docker or Podman to build Kali images inside a container without installing dependencies on the host. `build.sh` also gains `--hostname`, `--packages`, `--branch`, `--variant`, and `--arch` flags for customizing Kali installer images at build time.

— Names scripts and flags but no full example command shown

Kali Linux 2026.3 Release (Build-Script…

02 New NetHunter capabilities and device support NEW

75

Adds WearHunter, enabling control of a NetHunter watch from a phone via ADB over Wi-Fi or Bluetooth, including running commands and installing apps; NFC Arsenal, enabling reading, cloning, and editing of Mifare classic cards from the Kali chroot without an external adapter; KernelSU support, allowing installation of the generated installer zip via the KernelSU app with a patched kernel; wardriving support for the TicWatch Pro 3 series via an updated `libnexmonkali` library enabling internal monitor mode, compatible with the `aircrack-ng` suite, `kismet`, and other chroot tools; and 9 new NetHunter kernels covering Google Pixel on LineageOS 22.2/Android 15, Huawei P9 on EMUI8/LineageOS 16.0, LG K20 Plus on LineageOS 14.1, Moto G Stylus 5G 2022 on LineageOS 23.2, Nubia Z17 on LineageOS 22.2, POCO X5 5G/Redmi Note 12 5G on crDroid 12, Redmi Note 5 Pro on LineageOS 18.1, Sony Xperia 10 V on LineageOS 23.2, and Ulefone Armor 34+ on Android 16.

— Mechanism described but no exact commands given Capability and scope described, no usage walkthrough Install path named but no step-by-step detail Library and compatible tools

named, mechanism explained Device/OS list given, no install instructions

Kali Linux 2026.3 Release (Build-Script…

03 **New tools added to network repositories** NEW 65

Adds `dalfox` (XSS scanner), `katana` (crawling/spidering framework), `qsreplace` (query-string value replacer), `rustscan` (modern port scanner), `sdrangel` (Qt-based SDR front-end), and `snaffler-ng` (SMB share credential and sensitive data scanner) to the Kali network repositories.

— Tools and purposes named, no install command given

Kali Linux 2026.3 Release (Build-Script…

THINNER COVERAGE BELOW

04 **KDE Plasma updated to 6.7** IMPROVED 50

Updates KDE Plasma to 6.7, adding per-screen virtual desktops, network connection duplication, and performance/power optimizations for integrated Intel GPUs.

— Lists new Plasma features but no usage path Kali Linux 2026.3 Release (Build-Script…

05 **Kernel bumped to 7.1.5** IMPROVED 35

Updates the Kali kernel from 6.19 to 7.1.5 in the 2026.3 release.

— Only a version bump is stated, no change details

Kali Linux 2026.3 Release (Build-Script…

└──▷ ALSO FROM THESE RELEASES

WAS THIS USEFUL? 👍 👎

OTHER / UNCATEGORIZED

◆ UNCATEGORIZED

Lumia

Feedback ⓘ announced · Oct 26, 2026 BLOG ↗ RANK

Secure enterprise AI with Lumia's AI security platform. Govern employee AI usage, detect risks, and keep autonomous agents safely under control.

> Lumia added a Claude Compliance API integration, giving security teams visibility into Claude Enterprise conversations, file uploads, and agent activity, with optional inline enforcement.

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

01 **Claude Compliance API integration** NEW 57

Lumia adds support for Anthropic's Claude Compliance API, connecting Claude Enterprise to the Lumia platform without network infrastructure changes. This enables monitoring of Claude conversations, file uploads, and activity from tools such as Claude Code and Cowork through the Lumia AI Control Plane.

— Names the integration and monitored surfaces but no setup steps

launch-20261026-90d91f95

02 **Inline enforcement alongside Compliance API** NEW 30

Supports inline deployment alongside the Compliance API integration for real-time policy enforcement, blocking, redaction, and contextual user guidance.

— Describes enforcement capabilities without mechanism or config details

launch-20261026-90d91f95

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · October 26, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue