THE CYBER TOOLCHAIN

NO. 080

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED SEPTEMBER 20, 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

INFORMATION DENSITY

everything



BRIEFED | **EVERYTHING**

Every tool in the issue, in full.

all 50 changes

Do you prefer **scroll**? 👍 👎

▸ // **CONTENTS** SHOW 9 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.

IDENTIFY

See what an attacker with no credentials can reach in your AD

Attack-path discovery now starts from a null-session entry point and reports Tier-0 reachability, plus LDAP anonymous bind detection and CIS Benchmark mapping. That reproduces the actual opening move of most internal intrusions rather than assuming a compromised account, and the new `explain` command means a junior operator can read why a path matters instead of escalating it.

adscan

RESPOND

Get artifacts out of a disk image without the multi-pass wait

Both moved to a single-pass NTFS / APFS reader, so the image is walked once instead of re-read per artifact category — the difference between starting triage the same shift and starting it the next day. iLEAPP also picks up initial sysdiagnose parsing, and ALEAPP adds a parser for the Nova AI Chatbot app, a category of on-device app data that has had no standard extraction path.

ALEAPP · iLEAPP

RESPOND

Catch indicators an analyst typed into a case note

DFIR-IRIS integration now searches case notes for indicator matches, not just the structured IOC observable fields. Analysts routinely paste a hash or domain into narrative notes and never promote it to a formal observable, so prior-case hits were silently missed; the new no-key ScanMalware engine also means one fewer API key to provision before enrichment works.

Cyberbro

GOVERN

Pull a complete compliance dataset into Power BI instead of a truncated first page

The Power BI connector now paginates the API properly and ships more report dimensions plus a starter template, which ends the quiet failure mode where a dashboard silently reflected only the first page of findings. Library coverage extends to MITRE ATT&CK ICS /Mobile and the OWASP Agentic Top 10 , giving OT and AI-agent programs a framework to assess against.

CISO Assistant

◆ Exploitation & C2

adscan ⓘ v13.0.0 NOTES ↗ RANK

Free Active Directory pentesting tool for Linux, macOS and Windows. Automates AD and LDAP enumeration, Kerberoasting, ASREPRoast, password spraying, ADCS/ESC1, DCSync, RBCD, gMSA, shadow credentials, NTLM relay and credential dumping across 104 techniques, mapping BloodHound-compatible attack paths to Domain Admin.

> ADscan v13 adds zero-credential attack-path discovery starting from a null-session entry, an `explain` command with full teaching cards for every technique, LDAP anonymous bind detection, six host credential-protection checks, CIS Benchmark compliance mapping, and Tier-0 reachability reporting, while dropping Python 3.9 support and moving `adscan ci` behind the PRO tier.

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

01 **Targeted attack-path queries via --target** NEW 95

The `attack_paths` command gains a `--target` flag to query validated routes to one named group, host, or OU; it resolves the name to its canonical graph label and lists closest matches on a miss.

Focus attack-path output on a single high-value target — useful when you want to confirm whether any validated route reaches 'Domain Admins' without scrolling through the full path list.

```
$ attack_paths --target "Domain Admins"
```

— Names exact flag, resolution behaviour and runnable example. v13.0.0

02 **Technique teaching cards via explain command and learning mode**

NEW 90

New `explain` command renders a full teaching card for any technique in the coverage set — MITRE ATT&CK mapping, by-hand command, detection events, native check, and remediation. Learning mode now teaches the full technique set ADscan executes, including ADCS ESC2 through ESC17, coercion/relay techniques (PetitPotam, PrinterBug, DFSCoerce, coerce-and-relay to ADCS), named CVEs (Zerologon, noPac, EternalBlue, PrintNightmare), lateral-movement, DCSync, secret-dump, ACL-abuse, delegation escalations, and MSSQL escalations, via full teaching cards before execution and on demand through the `explain` command.

Pull up the full teaching card for a specific technique — MITRE mapping, by-hand command, detection events, and remediation — before executing it in a client

engagement.

```
$ explain
```

— Names command, exact techniques and CVEs, with example. v13.0.0

03 **Host-local credential-protection checks** NEW 90

Adds six host-local credential-protection checks collected over the same session on hosts where the scan account is a local administrator: LSASS `RunAsPPL`, WDigest cleartext caching, LM hash storage, LAN Manager auth level, minimum NTLM session security, and custom Security Support Providers; each carries GPO/registry remediation and a `Get-ItemProperty` validation step.

— Names all six checks and the validation command. v13.0.0

04 **LDAP Anonymous Bind Enabled finding** NEW 81

New first-class finding 'LDAP Anonymous Bind Enabled' with native remediation — disable anonymous operations via `dsHeuristics` and strip Anonymous Logon read grants — plus a validation bind that should fail after remediation.

— Names exact remediation mechanism and validation step. v13.0.0

05 **Graph scale visibility: graph_stats and pre-flight panel** NEW 76

New `graph_stats` command displays on-demand node/edge scale, control-hub density, and whether discovery will run in sampled mode; `adscan ci` now prints a one-line version. Attack-path discovery also shows a pre-flight panel before running with the same graph node/edge scale, control-hub density, and sampled-mode status.

Check graph scale and density instantly before kicking off a full attack-path discovery run on a large directory.

```
$ graph_stats
```

— Named command and example, mechanism clearly described. v13.0.0

06 **Tier-0 asset reachability reporting** NEW 70

Reports and the CLI now show which non-privileged accounts can reach a Tier-0 asset (domain controller, ADCS CA, Exchange server) and by what means: full local administrator, remote session, or database role.

— Describes scope and mechanism but no command shown. v13.0.0

07 **Compliance reporting: CIS Benchmark mapping and scorecard accuracy**

IMPROVED

68

Compliance reports now support mapping to the CIS Microsoft Windows Server Benchmark alongside ENS, NIS2, ISO 27001, DORA, and PCI DSS, version-aware to each host's actual Windows release (Server 2016/2019/2022/2025, Windows 10/11). The compliance scorecard now includes controls ADscan verified as correctly configured (conformant), not only broken ones; a control ADscan could not read stays 'not assessed' rather than assumed compliant.

— Names all frameworks and OS versions covered, no command. v13.0.0

---

08 **Per-workspace attack-path result caching** NEW

63

Attack-path results now persist per workspace and are skipped when using `--no-cache`; the cached set is invalidated automatically when the underlying graph changes.

— Names flag but gives no runnable example. v13.0.0

---

09 **Zero-credential attack paths from null session entry** IMPROVED

60

Zero-credential attack paths now begin at an explicit 'Unauthenticated (null session)' entry step, rated Critical when the chain reaches full domain compromise, so a zero-credential takeover no longer reports zero critical findings.

— Explains behaviour change but offers no command. v13.0.0

THINNER COVERAGE BELOW

10 **Python 3.10 minimum and adscan ci moved to PRO tier** BREAKING

57

Python 3.9 is no longer supported; the minimum supported Python version is now 3.10. `adscan ci` is now a PRO-only capability; LITE tier users must use the interactive `adscan start` workflow.

— Gives exact version cutoff and tier restriction, migration path noted. v13.0.0

---

11 **Reversible password encryption policy check** NEW

42

New configuration check flags domains or fine-grained password policies that store passwords with reversible encryption, with native remediation and validation.

— No named flag, command or mechanism given. v13.0.0

└──▷ BREAKING ON UPGRADE

! Python 3.9 is no longer supported; the minimum supported Python version is now 3.10.

! `adscan ci` is now a PRO-only capability; LITE tier users must use the interactive `adscan start` workflow.

v13.0.0 NOTES ↗ LATEST STABLE

ADscan v13 adds zero-credential kill chains, LDAP anonymous bind detection, host credential-protection checks, CIS Benchmark mapping, and targeted attack-path queries via `--target`.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v13.0.0 https://github.com/ADScanPro/adscan.git
# already have the repo? check out this version:
$ git checkout v13.0.0
```

└──▷ **TRY IT**

Focus attack-path output on a single high-value target — useful when you want to confirm whether any validated route reaches 'Domain Admins' without scrolling through the full path list.

```
$ attack_paths --target "Domain Admins"
```

Check graph scale and density instantly before kicking off a full attack-path discovery run on a large directory.

```
$ graph_stats
```

Pull up the full teaching card for a specific technique — MITRE mapping, by-hand command, detection events, and remediation — before executing it in a client engagement.

```
$ explain
```

› Adds `--target` flag to the `attack_paths` command to query validated routes to one named group, host, or OU — resolves the name to its canonical graph label and lists closest matches on a miss.

› Adds `--no-update` as an alias for `--no-update-check` to suppress launcher and runtime version checks in offline/air-gapped runs.

› Adds `graph_stats` command to display on-demand node/edge scale, control-hub density, and whether discovery will run in sampled mode; `adscan ci` prints a one-line version.

› Adds `explain` command to render a full teaching card — MITRE ATT&CK mapping, by-hand command, detection events, native check, and remediation — for any technique in the coverage set.

› Attack-path results now persist per workspace and are skipped on `--no-cache`; the cached set is invalidated automatically when the graph changes.

+9 more

└──▷ **BREAKING ON UPGRADE**

! Python 3.9 is no longer supported; the minimum supported Python version is now 3.10.

! `adscan ci` is now a PRO-only capability; LITE tier users must use the interactive `adscan start` workflow.

WAS THIS USEFUL? 👍 👎

◆ AI-Powered Offensive Security

PurpleAILAB Decepticon ⓘ v1.1.44 NOTES ↗ RANK

Autonomous Hacking Agent for Red Team

> Decepticon v1.1.44 introduces an Autohunt autonomous planning lane, adds AWS Bedrock and Kimi provider support, expands evidence and specialist validation controls, and now rejects default launcher credentials on startup.

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

01 Telemetry opt-out via environment variable NEW 80

Setting `DECEPTICON_TELEMETRY=off` disables telemetry sharing without going through the onboarding wizard; it can be set inline before `decepticon onboard` or persisted in a `.env` file so the opt-out applies to all future runs.

Disable telemetry at install time so no usage data is shared, without relying on the onboarding wizard prompt.

```
$ DECEPTICON_TELEMETRY=off decepticon onboard
```

Persist the telemetry opt-out across all future runs by setting it in the environment file the launcher reads.

```ini
DECEPTICON_TELEMETRY=off
```

— Exact env var, command and config file shown v1.1.44

THINNER COVERAGE BELOW

02 Autohunt autonomous planning lane NEW 55

A new Autohunt lane accepts an explicitly authorized target and validates planning documents and scope before marking an engagement ready, offered as an alternative to the default Soundwave interview-first planner.

— Names the lane and planner but no command or config given v1.1.44

03 Rejects default launcher credentials on startup BREAKING 55

Existing installations using default launcher credentials or missing secrets must update their configuration before starting — the release now rejects default credentials on

startup.

— Clear before/after but no exact config key named v1.1.44

04 **Executable specialist validation contracts** NEW 50

Adds executable specialist validation contracts covering capability contracts, evidence validation, lane scorecards, held-out evaluation fixtures, CVE-Bench dispatch plumbing, and pinned MITRE STIX bootstrapping.

— Lists named components but no usage path shown v1.1.44

05 **AWS Bedrock and Kimi provider support** NEW 45

Adds native AWS Bedrock default routes and Kimi for Coding provider support, including launcher onboarding for these providers.

— Names providers but no flags or commands supplied v1.1.44

06 **Evidence controls: local API ingestion, dependency reachability, severity ceilings**

NEW 40

Evidence controls gain local API ingestion, dependency reachability evidence, and severity ceilings.

— Named additions but no mechanism or config detail v1.1.44

07 **Dynamic workload teardown scoped by engagement and run** IMPROVED

30

Dynamic workload teardown is now scoped by engagement and run.

— States scope change but no mechanism or example v1.1.44

08 **Extra-header and streaming controls for provider calls** IMPROVED

25

Provider calls gain extra-header and streaming controls.

— Bare mention with no flag names or mechanism v1.1.44

09 **Typed finding-location guidance in skill catalog** NEW

25

Adds typed finding-location guidance in the skill catalog.

— Bare description with no further detail v1.1.44

└──▷ **BREAKING ON UPGRADE**

! Existing installations using default launcher credentials or missing secrets must update their configuration before starting — the release now rejects default credentials on startup.

v1.1.44 NOTES ↗ LATEST STABLE

Decepticon v1.1.44 adds Autohunt autonomous planning, AWS Bedrock and Kimi provider routes, and new evidence controls including severity ceilings and streaming.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v1.1.44
https://github.com/BitterSecurity/Decepticon.git
# already have the repo? check out this version:
$ git checkout v1.1.44
```

└──▷ **TRY IT**

Disable telemetry at install time so no usage data is shared, without relying on the onboarding wizard prompt.

```
$ DECEPTICON_TELEMETRY=off decepticon onboard
```

Persist the telemetry opt-out across all future runs by setting it in the environment file the launcher reads.

.env

```
DECEPTICON_TELEMETRY=off
```

- Adds `DECEPTICON_TELEMETRY=off` environment variable to disable telemetry sharing without going through the onboarding wizard.
- Adds Autohunt autonomous planning lane that accepts an explicitly authorized target and validates planning documents and scope before marking an engagement ready, separate from the default Soundwave interview-first planner.
- Adds native AWS Bedrock default routes and Kimi for Coding provider support, including launcher onboarding.
- Adds executable specialist validation contracts covering capability contracts, evidence validation, lane scorecards, held-out evaluation fixtures, CVE-Bench dispatch plumbing, and pinned MITRE STIX bootstrapping.
- Adds local API ingestion, dependency reachability evidence, and severity ceilings to evidence controls; provider calls gain extra-header and streaming controls; dynamic workload teardown is scoped by engagement and run.

+1 more

└──▷ **BREAKING ON UPGRADE**

! Existing installations using default launcher credentials or missing secrets must update their configuration before starting — the release now rejects default credentials on startup.

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ Web Application Security

humble ⓘ 1.66 NOTES ↗ RANK

A humble and fast security-oriented HTTP headers analyzer.

> humble 1.66 expands its detection database with a new fingerprint header and additional insecure header checks, and refines its Set-Cookie prefix validation.

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

01 **Improved Set-Cookie Invalid Prefixes check** IMPROVED

45

The `Set-Cookie: Invalid Prefixes` check now uses broader or more accurate detection logic.

— Names the exact check but not the new detection logic details. 1.66

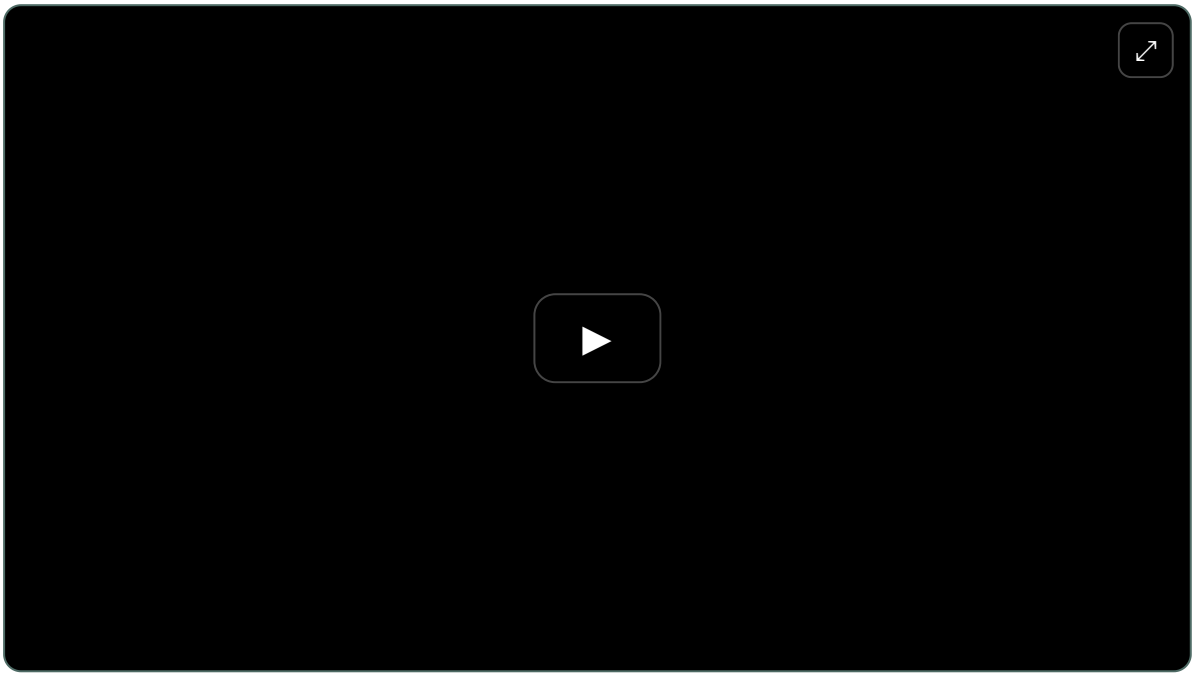
02 **Expanded fingerprint and insecure header detection** NEW

30

Adds 1 new fingerprint header to the detection database to assist server/software identification, and adds 2 new insecure header value checks to the deprecated/insecure checks suite.

— No specific header names or exact check identifiers given. 1.66

└──▷ ALSO FROM THESE RELEASES

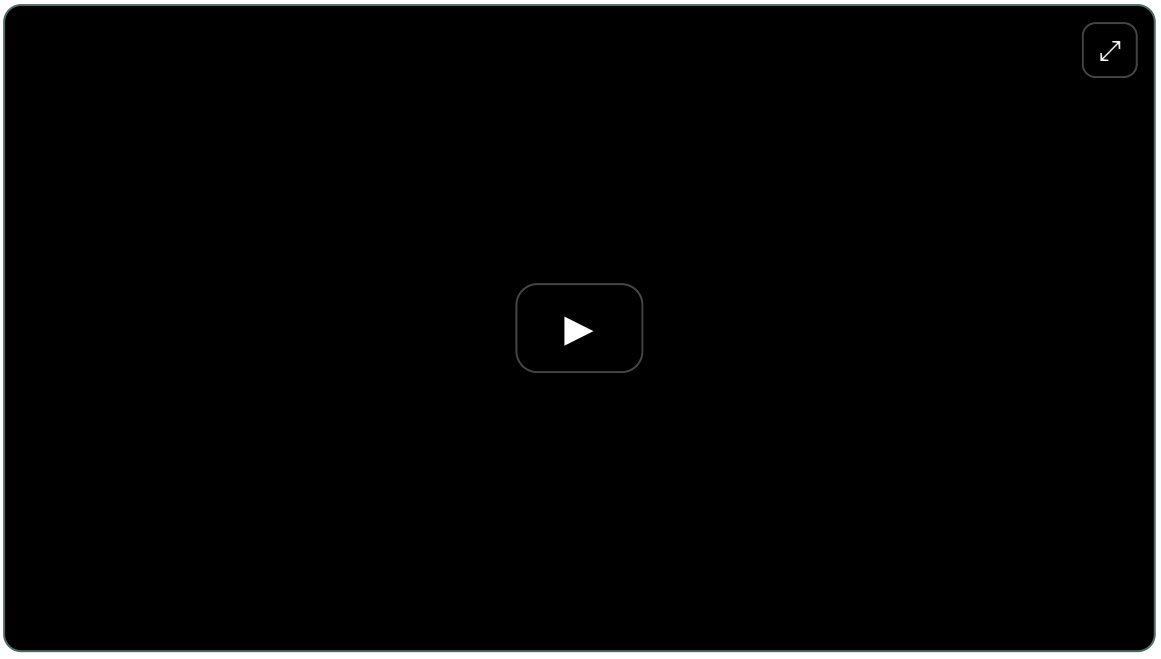


1.66 NOTES ↗ LATEST STABLE

humble 1.66 adds 1 new fingerprint header, 2 new insecure checks, and an improved 'Set-Cookie: Invalid Prefixes' check.

└──▷ **GET THIS VERSION**

```
$ git clone --branch 1.66 https://github.com/rfc-st/humble.git
# already have the repo? check out this version:
$ git checkout 1.66
```



- Adds 1 new fingerprint header to the detection database, expanding coverage to assist in server/software identification.
- Adds 2 new insecure header value checks to the deprecated/insecure checks suite.
- Improves the `Set-Cookie: Invalid Prefixes` check with broader or more accurate detection logic.

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

ALEAPP ⓘ v2026.4.1 NOTES ↗ CODE ↗ RANK

Android Logs Events And Protobuf Parser

> ALEAPP v2026.4.1 adds a forensic parser for the Nova AI Chatbot app and dramatically speeds up disk image processing with a new single-pass NTFS / APFS reader, alongside several under-the-hood performance and reporting improvements.

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

01 Single-pass NTFS/APFS reading via qnxprobe 1.30 IMPROVED

80

Reads NTFS and APFS disk images in a single pass using `qnxprobe` 1.30, cutting listing time for a 32 GB macOS E01 drive from 139.8 s to 8.5 s and a full run from 226.7 s to 85.7 s.

— Concrete before/after numbers and named tool version, no direct command v2026.4.1

02 Nova AI Chatbot forensic parser NEW

75

Adds forensic parser modules for Nova AI Chatbot (`com.scaleup.chatai`), covering conversation history, shared preferences, and user media submissions.

Parse a raw macOS E01 acquisition for Nova AI Chatbot artifacts — the single-pass APFS reader makes large images practical to process.

```
$ python aleapp.py -t raw -i /evidence/macbook.E01 -o
/reports/nova_case/
```

— Names package and artifact types, includes runnable command v2026.4.1

03 Per-artifact LAVA database commits IMPROVED

60

Commits the LAVA database once per artifact instead of once per staged file, cutting processing of a 4,000-message WhatsApp artifact from 20.6 s to 9.5 s.

— Clear before/after metric but no user-facing action v2026.4.1

THINNER COVERAGE BELOW

04 ArtifactResult streaming path for large artifacts NEW

40

Adds `ArtifactResult`, a streaming result path intended for handling large artifacts more efficiently.

— Named surface but mechanism and impact left vague v2026.4.1

05 **Summarized view for oversized HTML report tables** IMPROVED 40

Oversized HTML report tables are held back and replaced with a summarized view instead of rendering an unbounded table.

— Describes behavior change but no threshold or config named v2026.4.1

06 **Evidence-relative source path recording** IMPROVED 25

Records evidence-relative source paths for directory and single-file inputs.

— Bare description with no mechanism or usage detail v2026.4.1

v2026.4.1 NOTES ↗ CODE ↗ LATEST STABLE

ALEAPP v2026.4.1 adds a Nova AI Chatbot forensic parser and dramatically speeds up NTFS / APFS image reads with qnxprobe 1.30.

└──▷ GET THIS VERSION

```
$ git clone --branch v2026.4.1
https://github.com/abrignoni/ALEAPP.git
# already have the repo? check out this version:
$ git checkout v2026.4.1
```

└──▷ TRY IT

Parse a raw macOS E01 acquisition for Nova AI Chatbot artifacts — the single-pass APFS reader makes large images practical to process.

```
$ python aleapp.py -t raw -i /evidence/macbook.E01 -o
/reports/nova_case/
```

- Adds forensic parser modules for Nova AI Chatbot (`com.scaleup.chatai`), including conversation history, shared preferences, and user media submissions.
- Reads NTFS and APFS disk images in a single pass using `qnxprobe` 1.30 — listing a 32 GB macOS E01 drops from 139.8 s to 8.5 s, and a full run from 226.7 s to 85.7 s.
- Adds `ArtifactResult`, a streaming result path for handling large artifacts more efficiently.

- Commits the LAVA database once per artifact instead of once per staged file, cutting a 4,000-message WhatsApp artifact from 20.6 s to 9.5 s.
- Records evidence-relative source paths for directory and single-file inputs.

+1 more

WAS THIS USEFUL? 👍 👎

iLEAPP ⓘ v2026.4.2 NOTES ↗ CODE ↗ RANK

iOS Logs, Events, And Plist Parser

> iLEAPP added initial sysdiagnose parsing support, moved to single-pass NTFS / APFS image reads via qnxprobe 1.30, and made several smaller improvements to media artifact reporting and internal processing performance.

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

01 **Single-pass NTFS/APFS image reads via qnxprobe 1.30** IMPROVED 65

Reads NTFS and APFS images in one pass using qnxprobe 1.30, replacing the previous multi-pass approach.

– Clear before/after and named tool version, but no user-facing action v2026.4.2

02 **Keyboard Input Contexts chat decoding** NEW 65

Decodes chat type and party from Keyboard Input Contexts identifiers, scoped to the Messenger `_0` form.

– Names the exact scoped form but no report field or output location given v2026.4.2

THINNER COVERAGE BELOW

03 **Initial sysdiagnose parsing support** NEW 55

Adds initial sysdiagnose parsers, including PowerLog database reads inside packed sysdiagnoses and AppleDouble sidecar filtering from sysdiagnose readers.

– Names artifacts parsed but no usage path or command given v2026.4.2

04 **Media artifact handling for Calculator Vault and Photos face crops**

IMPROVED 55

Calculator Vault videos are now surfaced as proper media artifacts, looked up in their own album folder, and Photos.sqlite face crops are reported as media instead of a raw report folder path.

– Describes two related media-reporting fixes without exact report field names v2026.4.2

05 **LAVA database commit batching** IMPROVED 45

Commits the LAVA database once per artifact instead of once per staged file, improving write performance.

– Explains the change but it is purely internal with no user action v2026.4.2

06 **Evidence-relative source path recording** IMPROVED 30

Records evidence-relative source paths for directory and single-file inputs.

— One-line description with no mechanism or output detail v2026.4.2

07 **Mobile Installation log deduplication** IMPROVED 30

Deduplicates Mobile Installation log lines reported across multiple files.

— Names the artifact but not the mechanism or scope of dedup v2026.4.2

08 **Archive member deduplication for zip and tar staging** IMPROVED 30

Stages zip and tar member names stored more than once as a single file.

— Thin one-line internal staging fix with no further detail v2026.4.2

v2026.4.2 NOTES ↗ CODE ↗ LATEST STABLE

iLEAPP v2026.4.2 adds sysdiagnose parsing, Snapchat Memories, NTFS / APFS single-pass image reads, and Calculator Vault/Photos media handling.

└──▷ GET THIS VERSION

```
$ git clone --branch v2026.4.2
https://github.com/abrignoni/iLEAPP.git
# already have the repo? check out this version:
$ git checkout v2026.4.2
```

- Adds initial sysdiagnose parsers, including PowerLog database reads inside packed sysdiagnoses and AppleDouble sidecar filtering from sysdiagnose readers.
- Reads NTFS and APFS images in one pass with qnxprobe 1.30, replacing the previous multi-pass approach.
- Adds Calculator Vault videos as proper media artifacts, looked up in their own album folder.
- Reports Photos.sqlite face crops as media instead of a raw report folder path.
- Commits the LAVA database once per artifact instead of once per staged file, improving write performance.

+4 more

WAS THIS USEFUL? 👍 👎

◆ Threat Intelligence

Cyberbro ⓘ v0.15.0 NOTES ↗ RANK

A simple application that extracts your IoCs from garbage input and checks their reputation using multiple CTI services.

> Cyberbro v0.15.0 adds a new no-key ScanMalware analysis engine and extends DFIR-IRIS integration to search case notes for indicator matches, not just structured IOC observables.

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

01 **DFIR-IRIS case note searching** NEW 75

New `DFIR_IRIS_SEARCH_NOTES` environment variable/config setting (default `false`) enables searching for indicator matches inside DFIR-IRIS case notes in addition to IOC observables. When enabled, analysis results return hits from both notes and IOC observables, useful when analysts record indicators in free-text notes rather than structured IOC fields. Set via `.env` as `DFIR_IRIS_SEARCH_NOTES=true`.

Enable DFIR-IRIS note searching so Cyberbro queries case notes when enriching observables.

env

```
DFIR_IRIS_SEARCH_NOTES=true
```

Enable note searching in DFIR-IRIS to surface IOC context buried in case notes during an investigation.

env

```
DFIR_IRIS_SEARCH_NOTES=true
```

Enable note-level indicator searches in DFIR-IRIS so triage returns hits from both case notes and IOC observables — useful when analysts record indicators in free-text notes rather than structured IOC fields.

env

```
DFIR_IRIS_SEARCH_NOTES=true
```

Enable DFIR-IRIS note searching to surface case notes during indicator lookups.

```env
DFIR_IRIS_SEARCH_NOTES=true
```

— Names exact env var, default, and behaviour change. v0.15.0

02 **ScanMalware analysis engine** NEW 60

Adds a `scanmalware` engine that queries the ScanMalware archive of sandboxed URL scans for `domain`, `URL`, and `IP` observable types. No API key is required (`free_no_key`).

— Names engine key and supported observable types, no usage example. v0.15.0

v0.15.0 NOTES ↗ LATEST STABLE

Cyberbro v0.15.0 adds a ScanMalware engine and updates DFIR-IRIS search integration.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v0.15.0
https://github.com/stanfrbd/cyberbro.git
# already have the repo? check out this version:
$ git checkout v0.15.0
```

› Adds `ScanMalware` as a new analysis engine for indicator lookups.

› Updates the DFIR-IRIS search integration with new search capabilities.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Secure Access (VPN / SASE / ZTNA)

Termius ⓘ 10.1.0 (2026-09-21) BLOG ↗ RANK

This page introduces the core concepts of Termius, including Vaults, Groups, Hosts, Keychain, and Terminal, and explains how they work together to organize infrastructure access.

> Termius 10.1.0 removes the paywall on several connection features, making Proxy, Agent Forwarding, Host Chains, and Serial connections free for all users.

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

01 **Proxy, Agent Forwarding, Host Chains, Serial now free** IMPROVED

45

Proxy, Agent Forwarding, Host Chains, and Serial connections, previously paid features, are now available on the free tier.

— Names four features unlocked but no mechanism or limits given. 10.1.0 (2026-09-21)

10.1.0 (2026-09-21) BLOG ↗ LATEST STABLE

Termius 10.1.0 makes Proxy, Agent Forwarding, Host Chains, and Serial connections free for all users.

› Proxy, Agent Forwarding, Host Chains, and Serial connections are now available on the free tier.

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

Didit ⓘ snapshot-20260920 NOTES ↗ RANK

Didit provides identity verification, fraud prevention, and transaction-monitoring APIs, SDKs, and MCP tools.

> Didit added camera control options across its Web SDK and direct verification URLs, and introduced national ID-number lookup plus digital ID wallet sign-in on native SDK entry screens.

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

01 Camera control options in Web SDK and verification URLs NEW

78

Adds `defaultDocumentCamera`, `defaultLivenessCamera`, `showDocumentCameraSwitchButton`, and `showLivenessCameraSwitchButton` options to the web SDK (`@didit-protocol/sdk-web` 0.4.0), matching camera controls already available in native SDKs. Also adds `liveness_camera` and `liveness_camera_switch` query parameters to the direct verification URL, letting integrators lock the camera and hide the in-capture switcher without using the SDK (e.g. `https://verify.didit.me/session/<session-id>?liveness_camera=back&liveness_camera_switch=false`).

Lock a kiosk or operator-facing device to the rear camera for liveness capture and hide the in-capture switcher so the user cannot switch lenses.

```
$ https://verify.didit.me/session/<session-id>?
liveness_camera=back&liveness_camera_switch=false
```

— Names exact flags and query params with a runnable example URL. snapshot-20260920

THINNER COVERAGE BELOW

02 National ID lookup and digital ID wallet sign-in NEW

55

Adds national ID-number lookup and digital ID wallet sign-in as verification methods on the native SDK entry screen (iOS, Android, React Native, Flutter 4.8.0), with on-device field validation and optional fallback to document capture.

— Explains mechanism and platforms but no config key or command shown. snapshot-20260920

snapshot-20260920 NOTES ↗ LATEST STABLE

Web SDK 0.4.0 gains camera control options; Mobile SDKs 4.8.0 add national ID-number lookup and digital ID wallet sign-in on native entry screens.

└──▷ **TRY IT**

Lock a kiosk or operator-facing device to the rear camera for liveness capture and hide the in-capture switcher so the user cannot switch lenses.

```
$ https://verify.didit.me/session/<session-id>?
liveness_camera=back&liveness_camera_switch=false
```

- Adds `defaultDocumentCamera`, `defaultLivenessCamera`, `showDocumentCameraSwitchButton`, and `showLivenessCameraSwitchButton` options to the web SDK (`@didit-protocol/sdk-web` 0.4.0), matching the camera controls already available in native SDKs.
- Adds `liveness_camera` and `liveness_camera_switch` query parameters to the direct verification URL for camera control without the SDK.
- Adds national ID-number lookup and digital ID wallet sign-in as verification methods on the native SDK entry screen (iOS, Android, React Native, Flutter 4.8.0), with on-device field validation and optional fallback to document capture.

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

CISO Assistant ⓘ v4.0.5 NOTES ↗ RANK

CISO Assistant is a one-stop-shop GRC platform for Risk Management, AppSec, Compliance & Audit, TPRM, BIA, Privacy, and Reporting. It supports 200+ global frameworks with automatic control mapping, including ISO 27001, NIST CSF, SOC 2, CIS, PCI DSS, NIS2, DORA, GDPR, HIPAA, CMMC, and more.

> CISO Assistant's Power BI connector gained proper API pagination for full dataset retrieval, more report dimensions, and a ready-to-use starter template, while the core platform added MITRE ATT&CK ICS /Mobile and OWASP Agentic Top 10 library coverage, findings integration in tasks and requirement assessments, and several UI additions including a mini graph explorer, tabular mapping view, and an expanded command palette.

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

01 Power BI connector pagination, dimensions, starter template

IMPROVED 80

Adds proper API pagination to the Power BI connector, enabling full dataset retrieval across large CISO Assistant instances, and expands available dimensions in the connector for richer reporting coverage. Ships a `CisoAssistant-starter.pbit` starter report template with every connector release, requiring only an instance URL entered as `BaseUrl` on first open in Power BI Desktop.

Connect Power BI Desktop to your CISO Assistant instance for the first time using the starter template.

> 📍 1. Install the connector per automation/powerbi/README.md and trust the signing certificate thumbprint AAB77C4E62D72D26F1E05AAA46457D90A653541E (see signing/trust-thumbprint.md). 2. Open CisoAssistant-starter.pbit in Power BI Desktop. 3. When prompted, enter your instance URL as the value for BaseUrl (e.g. `https://your-instance.example.com`). 4. Click Load — the connector will now paginate through the full API dataset automatically.

— Names exact template file, config field, and setup steps `powerbi-v1.1.0` `v4.0.5`

THINNER COVERAGE BELOW

02 Findings tab and picker in tasks and assessments NEW

50

Adds a findings tab to the task detail view, and enables picking existing findings when performing a requirement assessment.

— Names UI surfaces but no exact navigation steps v4.0.5

03 **New framework libraries: MITRE ATT&CK ICS/Mobile and OWASP Agentic Top 10**

NEW 45

Adds MITRE ATT&CK library coverage for ICS and mobile platforms, and adds OWASP Top 10 for Agentic Applications 2026 as a new library.

— Names two frameworks but no usage steps v4.0.5

04 **Mini graph explorer and visual domains mode** NEW 40

Introduces a mini graph explorer and an experimental visual mode for domains management.

— Names features but experimental status with no usage detail v4.0.5

05 **Workflow enablers for evidences, tasks, and metrics** IMPROVED 40

Extends workflow enablers to cover evidences, tasks, and metrics use cases.

— Names three use cases but no mechanism detail v4.0.5

06 **Tabular mode for mapping views** NEW 30

Adds tabular mode for viewing mapping data.

— Single-line description with no scope detail v4.0.5

07 **Alternate rendering modes for breakdown charts** NEW 30

Adds alternate rendering modes for breakdown charts.

— Bare description, no modes named v4.0.5

08 **Additional OIDC scopes in SSO configuration** IMPROVED 25

SSO configuration now supports additional OIDC scopes.

— Bare mention, no specific scopes listed v4.0.5

09 **Expanded command palette search** IMPROVED 20

Extends the command palette with more capabilities and broader search coverage.

— Vague, no specifics on new capabilities v4.0.5

v4.0.5 NOTES ↗ LATEST STABLE

CISO Assistant v4.0.5 adds MITRE ATT&CK for ICS/Mobile, OWASP Agentic Top 10 , tabular mapping, mini graph explorer, and extended SSO scopes.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v4.0.5 https://github.com/intuitem/ciso-assistant-community.git
# already have the repo? check out this version:
$ git checkout v4.0.5
```

- Supports additional OIDC scopes in SSO configuration.
- Adds MITRE ATT&CK library coverage for ICS and mobile platforms.
- Adds OWASP Top 10 for Agentic Applications 2026 as a library.
- Adds a findings tab to the task detail view.
- Enables picking existing findings when performing a requirement assessment.

+6 more

powerbi-v1.1.0 NOTES ↗ STABLE

CISO Assistant Power BI connector gains proper API pagination and additional report dimensions.

└──▷ **GET THIS VERSION**

```
$ git clone --branch powerbi-v1.1.0 https://github.com/intuitem/ciso-assistant-community.git
# already have the repo? check out this version:
$ git checkout powerbi-v1.1.0
```

└──▷ **HOW TO FIND IT**

Connect Power BI Desktop to your CISO Assistant instance for the first time using the starter template.

📍 1. Install the connector per automation/powerbi/README.md and trust the signing certificate thumbprint AAB77C4E62D72D26F1E05AAA46457D90A653541E (see signing/trust-thumbprint.md). 2. Open CisoAssistant-starter.pbit in Power BI Desktop. 3. When prompted, enter your instance URL as the value for BaseUrl (e.g. `https://your-instance.example.com`). 4. Click Load — the connector will now paginate through the full API dataset automatically.

- Adds proper API pagination to the Power BI connector, enabling full dataset

retrieval across large CISO Assistant instances.

- Expands available dimensions in the Power BI connector for richer reporting coverage.
- Ships `CisoAssistant-starter.pbit` starter report template with every connector release, requiring only an instance URL entered as `BaseUrl` on first open.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · September 20, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe