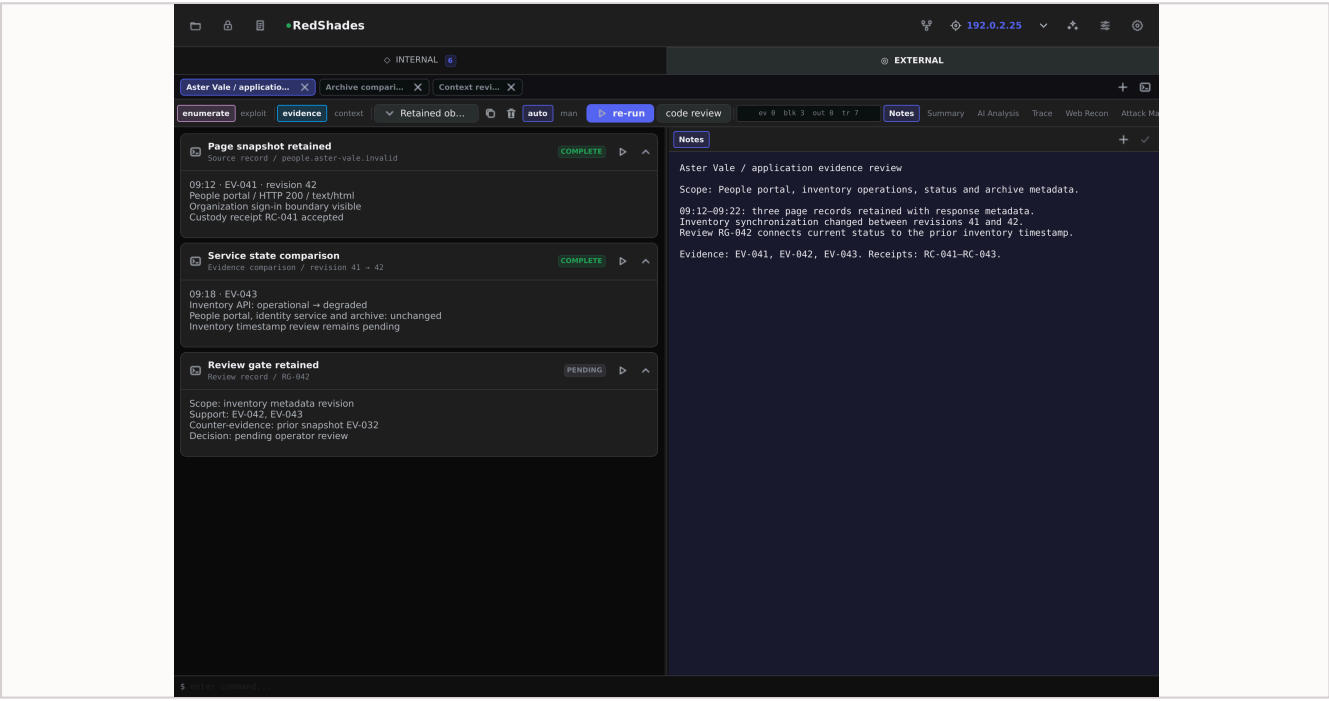
PLATFORM SCOPE

Put models to work. Keep software in control.

Long technical investigations ask more of a system than a good answer. RedShades gives smaller, specialized models defined decisions while deterministic software owns scheduling, evidence, policy and recovery. A native workspace brings those decisions, their sources and the tools behind them into view.



Keep source notes, context and investigation progress together.

The investment thesis is integration: useful work can accumulate across model sessions, tool changes and runtime replacement. The architecture supports that thesis; comparative model cost and reliability still require controlled measurement.

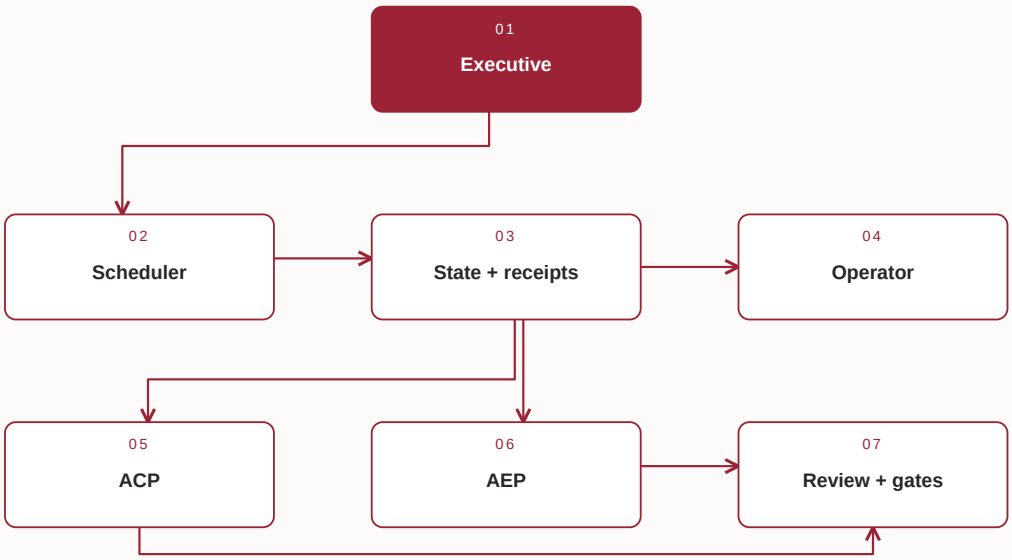
Implemented

Platform scope

EVIDENCE-DRIVEN SCHEDULING

The next step is a software decision

Each stage declares the evidence it needs. The scheduler advances eligible branches and revisits waiting work when observations change. Models interpret uncertain inputs; they do not have to reconstruct the workflow or remember which branch can run.



01 → 02 · observes / routes
02 → 03 · evaluates / commits
03 → 04 · projects
03 → 05 · capability gap
03 → 06 · software incident
05 → 07 · candidate
06 → 07 · repair evidence

Evidence-driven scheduling · overview.

The Executive supervises progress. Capability development and software repair have separate owners, so a stalled investigation can be routed to the appropriate kind of work. Child investigations retain their scope, parent context and completion relationship.

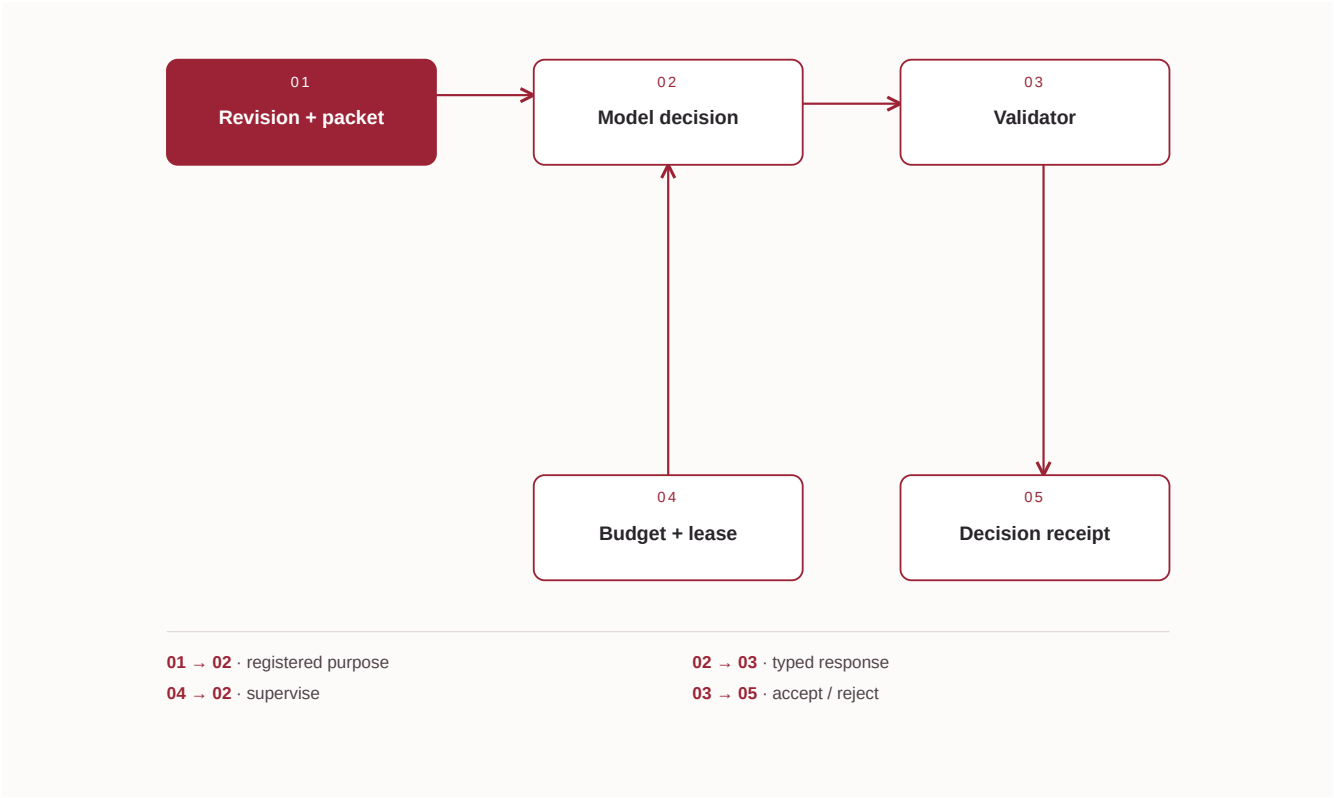
Implemented

Evidence-driven scheduling

MODEL ALLOCATION

Spend intelligence on the uncertain part

Scheduling, state, policy and validation are software responsibilities. Interpretation and synthesis are model responsibilities. That division gives a small specialist a complete, bounded job instead of asking it to manage an entire engagement.



Model allocation · overview.

The 70% deterministic / 30% neural framing describes the design philosophy. It is not a measured share of code, runtime or success. Model economics remain a question for controlled evaluation.

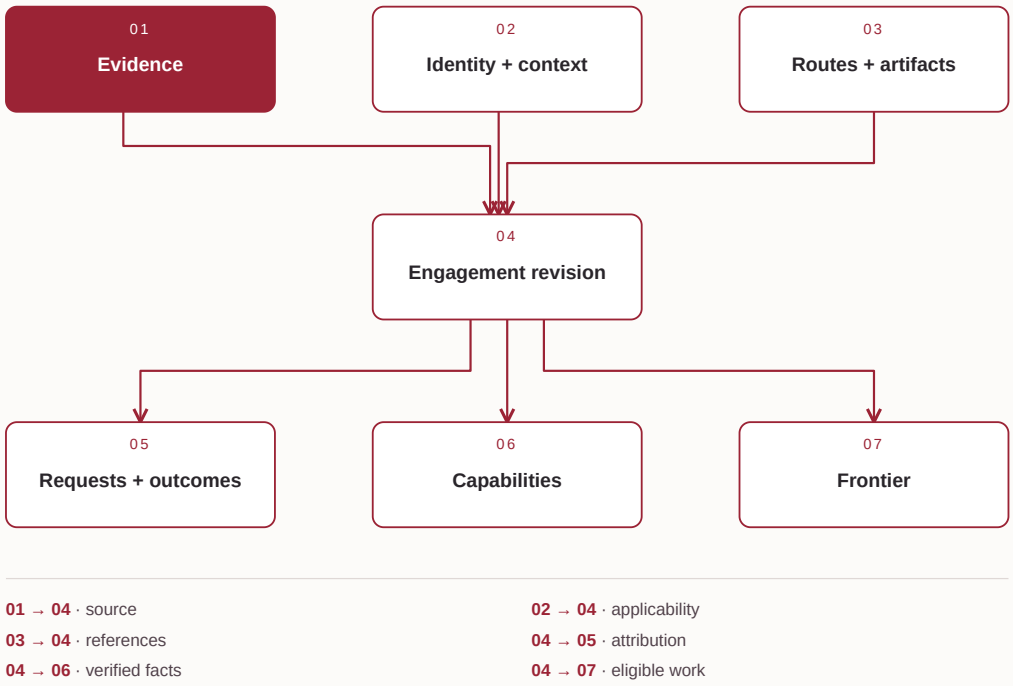
Design philosophy

Model allocation

SHARED ENGAGEMENT STATE

Memory belongs to the engagement

Versioned records link observations, identities, routes, artifacts and outcomes. A new model session or replacement worker can read the accepted state and its sources without rebuilding the investigation from a conversation.



Shared engagement state · overview.

The scheduler and native views draw on the same records. Revision references identify the inputs behind a decision; they also make stale results distinguishable from current work.

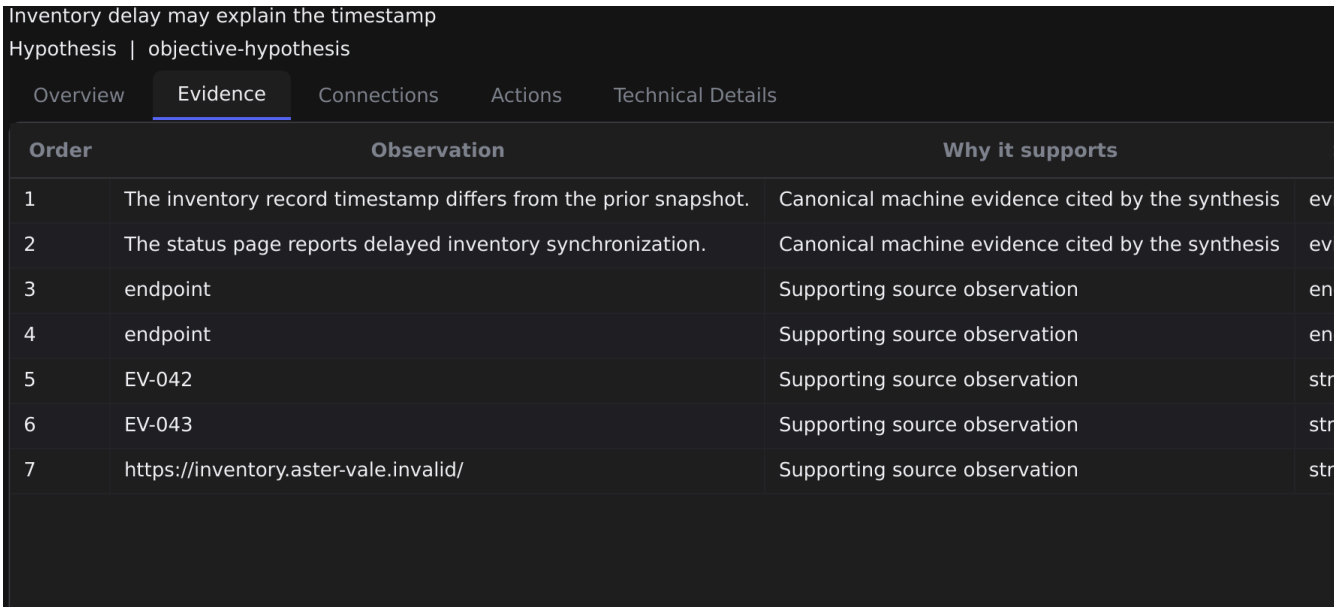
Implemented

Shared engagement state

EVIDENCE ATTRIBUTION

A finding should lead back to its source

A tool result retains its source, context and interpretation. Later stages can reuse it, and an operator can inspect what actually supported a conclusion. Competing observations remain distinguishable until there is evidence to resolve them.



Inspect the source records supporting the selected finding.

Attribution is the connection between tool integration and model quality: a specialist receives inspectable material with context, rather than an untraceable summary.

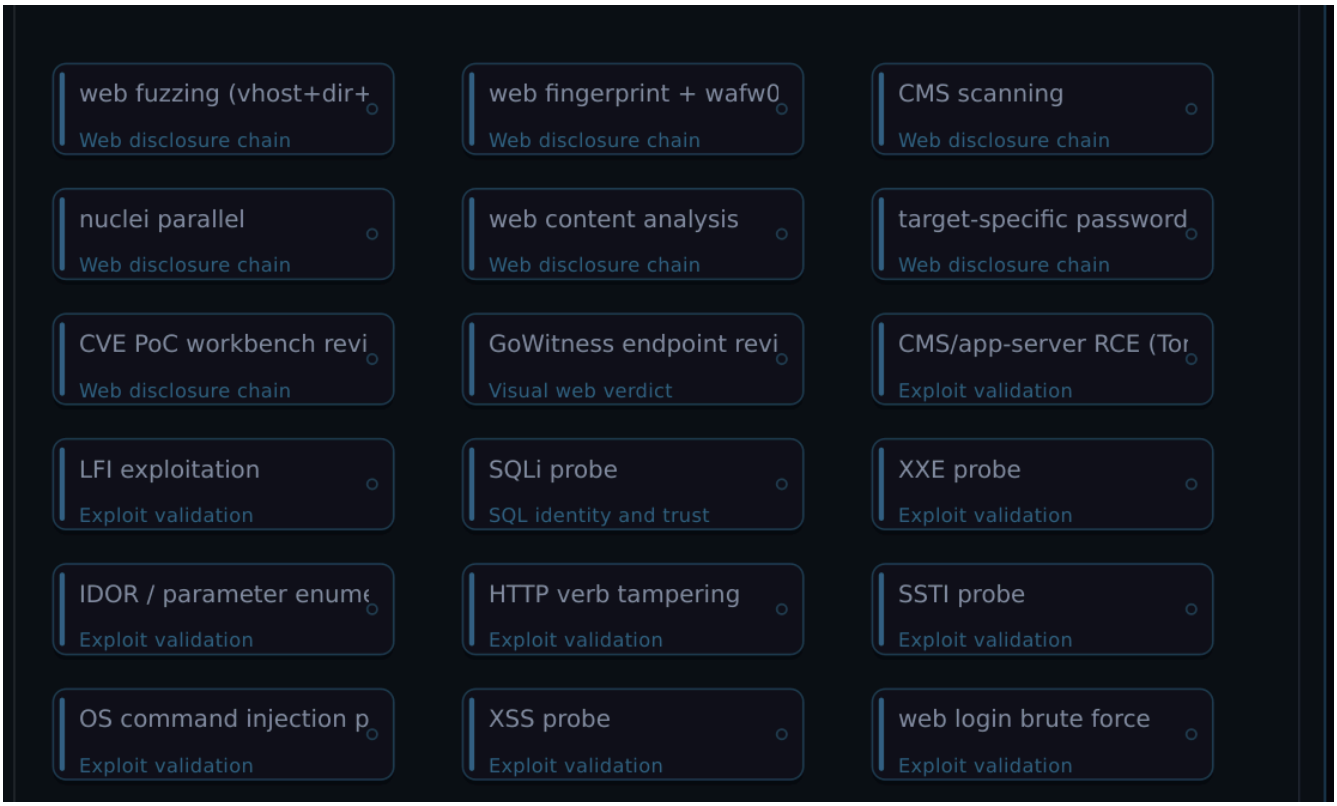
Implemented

Evidence attribution

CONDITIONAL STAGE COVERAGE

A repertoire, selected by evidence

The Validated Core contains 88 conditional stages spanning discovery, service and identity analysis, web investigation, artifacts and reporting. Thirteen C2 continuation stages add shared and platform-specific session work.



Web investigation within the 198-stage repertoire.

Prerequisites, platform context and policy determine the path. The atlas identifies the available responsibilities; its order does not prescribe an execution sequence.

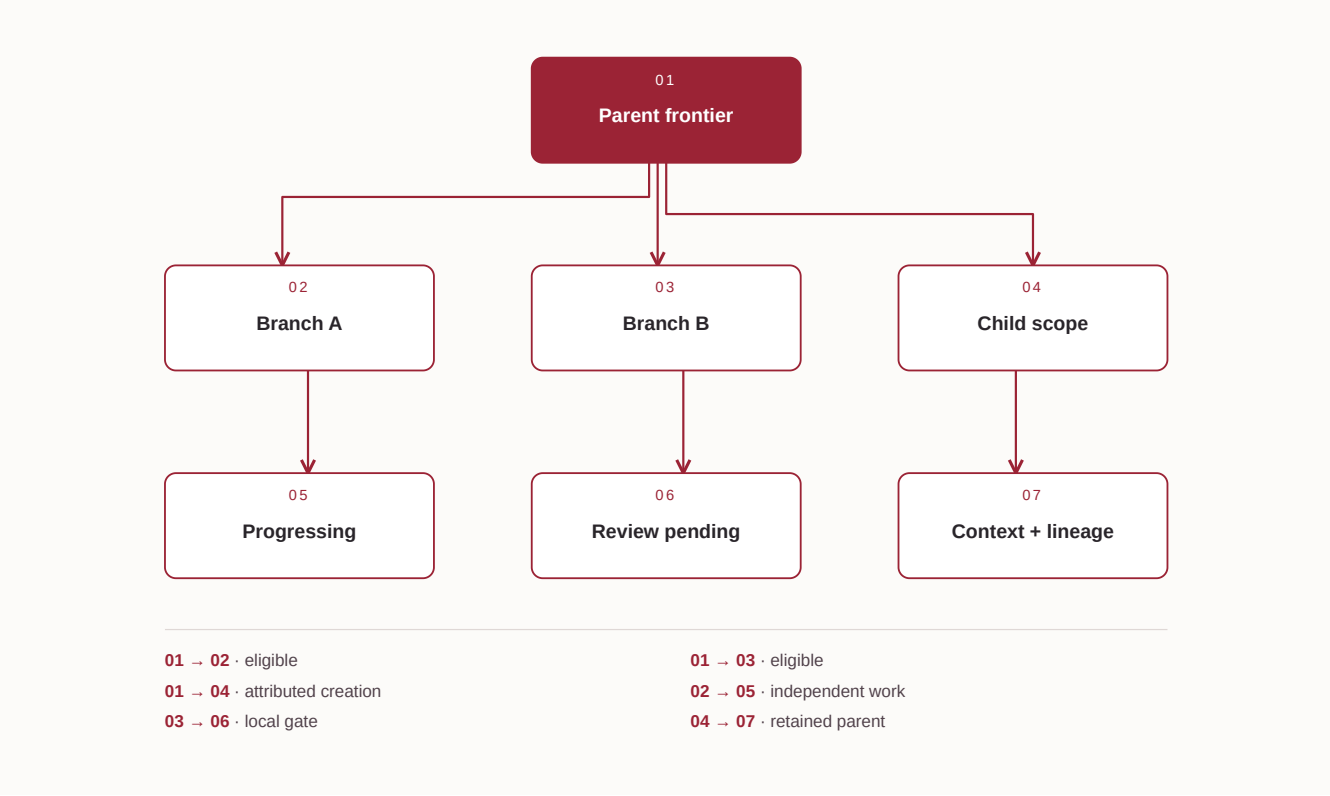
Implemented

Conditional stage coverage

BRANCH-LOCAL PROGRESS

A local question need not stop the run

An endpoint review or missing identity fact can hold one branch while unrelated work continues. A global pause is an explicit operator decision with a different scope.



Branch-local progress · overview.

Waiting work retains the input that could make it eligible. New observations can reopen useful branches without turning every unresolved item into a retry loop.

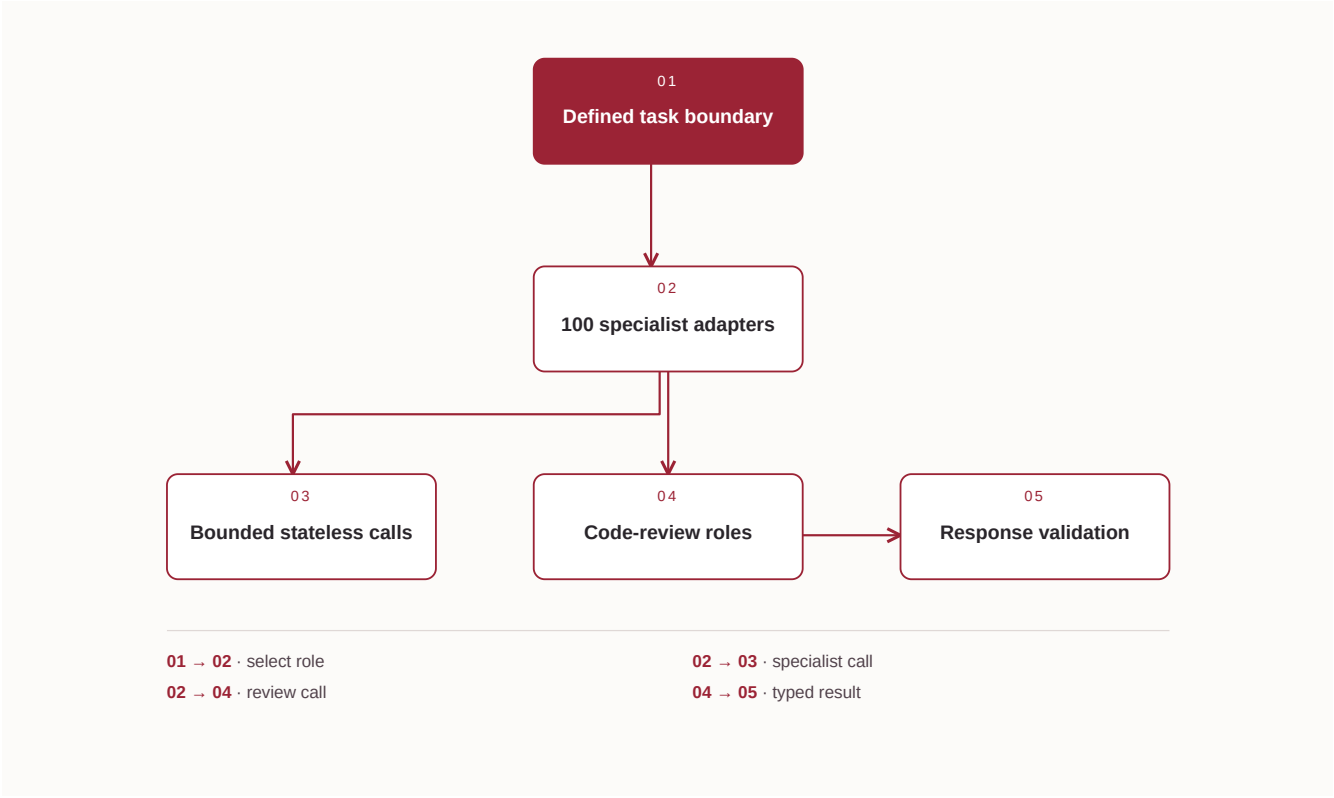
Implemented

Branch-local progress

BOUNDED MODEL CALLS

A complete job for a specialist

Core includes 100 fine-tuned specialist adapters for bounded stateless calls and code-review roles. Each call receives a defined purpose and structured evidence. Software validates its response and retains the accepted result with model attribution.



Bounded model calls · overview.

Capacity, token accounting and response limits surround the call. The task boundary selects the specialist; the engagement keeps the evidence and review history.

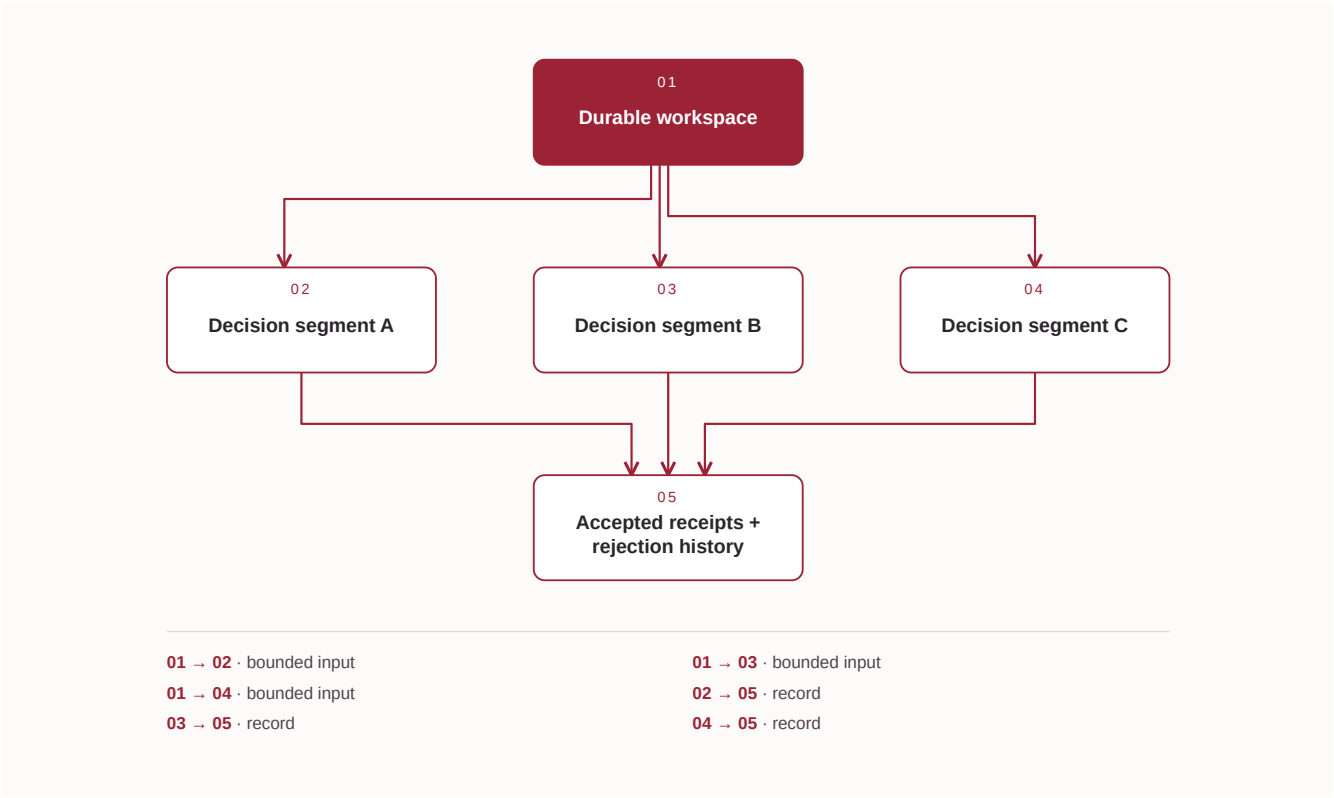
Core model entitlement

Bounded model calls

PERSISTENT MODEL SESSIONS

Harder work needs a persistent workspace

The fine-tuned 30B3A Flash model supports persistent higher-complexity sessions. Executive, capability-development and repair workspaces carry accepted artifacts, prior review and progress between segments.



Persistent model sessions · overview.

Access to fine-tuned models and specialist adapters follows controlled subscription gates. Weekly model credits and selective weights entitlements support different deployment needs; the bundle comparison sets out those terms.

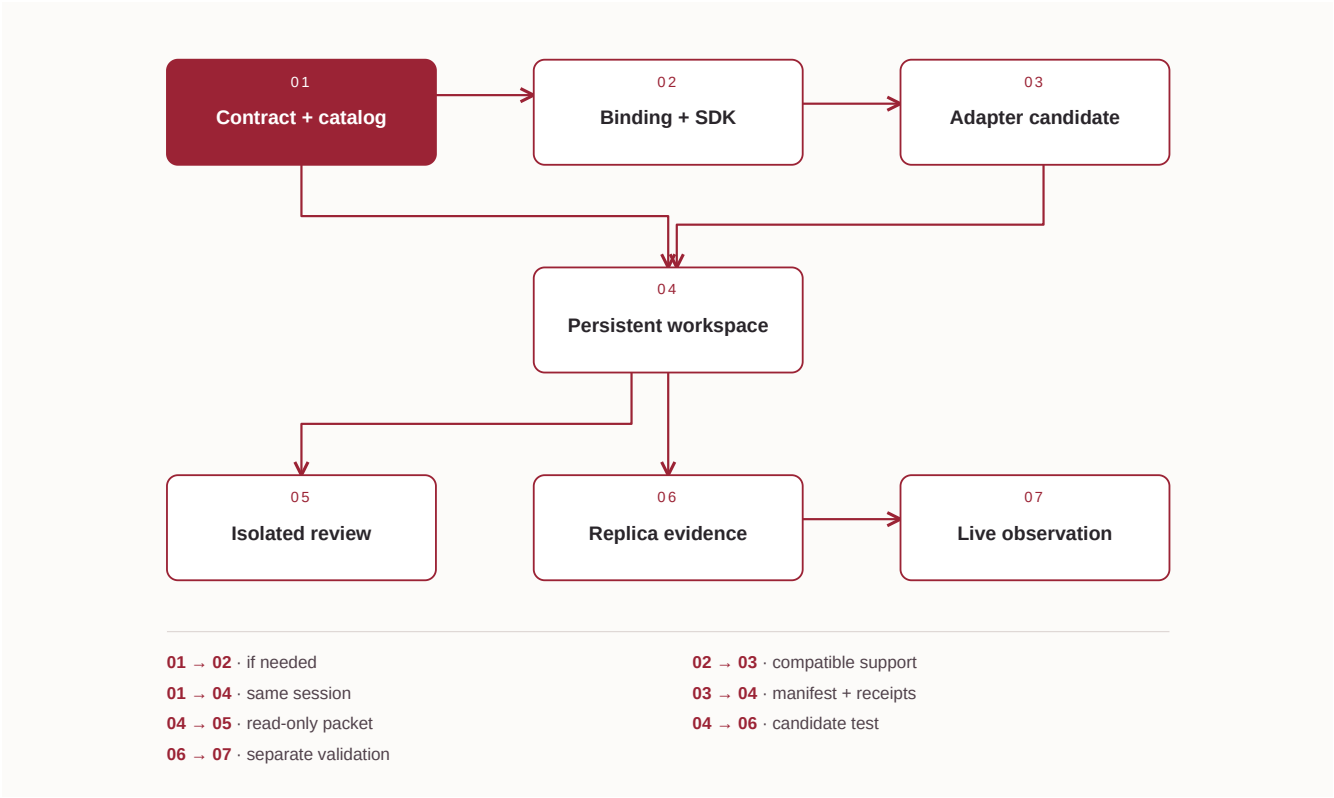
Advanced model entitlement

Persistent model sessions

CAPABILITY DEVELOPMENT

Build the missing interaction against a contract

The Adaptive Capability Pipeline (ACP) is an adaptive capability-generation harness. It develops candidates from observed evidence and source mechanics, retaining the contract through binding, SDK selection, adapter generation, review and replica validation.



Capability development · overview.

A compatible catalog artifact or SDK can remove unnecessary generation work. New candidates retain their correction history and supporting artifacts for review.

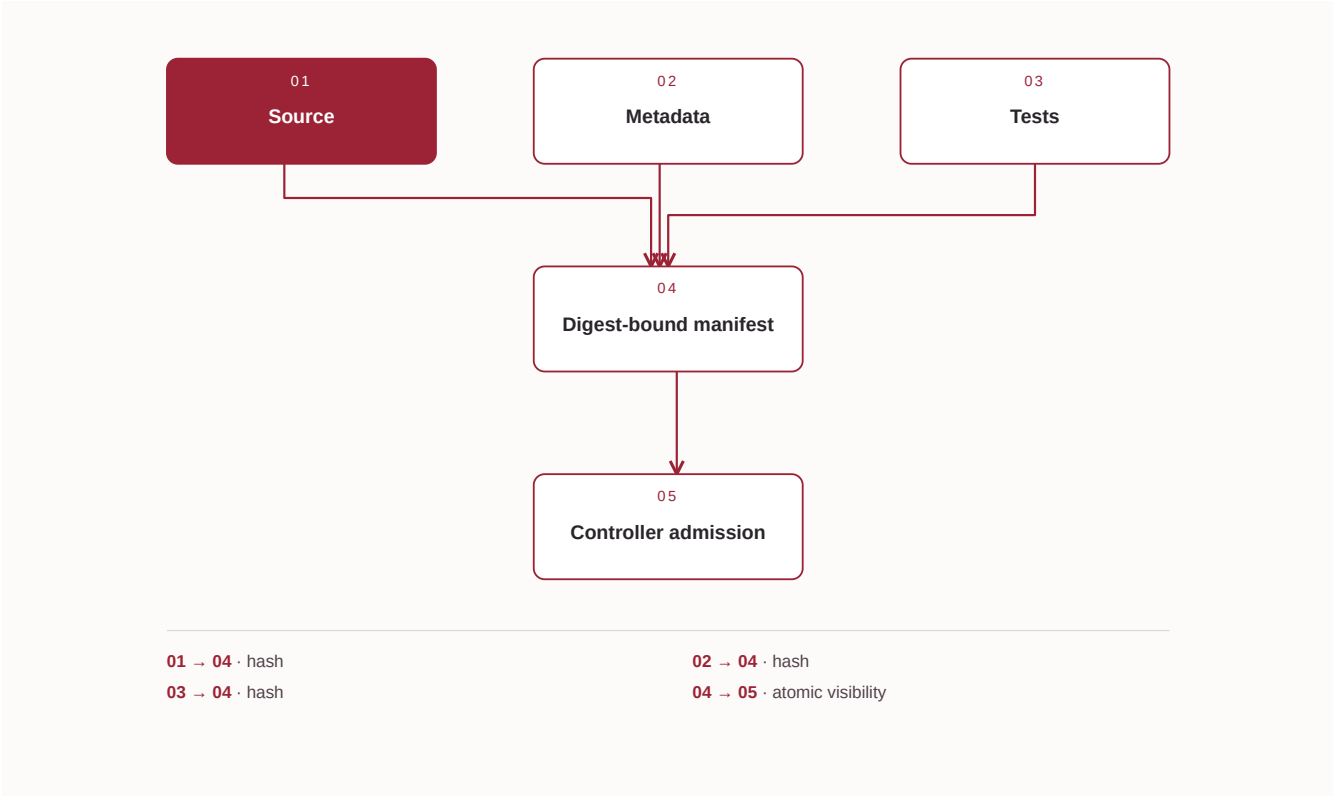
Implemented

Capability development

CANDIDATE PUBLICATION

Generated code needs an admission boundary

Source findings and advisories can inform a typed capability candidate. Source, metadata and tests are published together with their digests, giving review a specific artifact set to examine.



Candidate publication · overview.

The workbench can retain a candidate for controlled evaluation when a ready-made implementation is absent. Publication establishes artifact identity; admission determines whether it can be used.

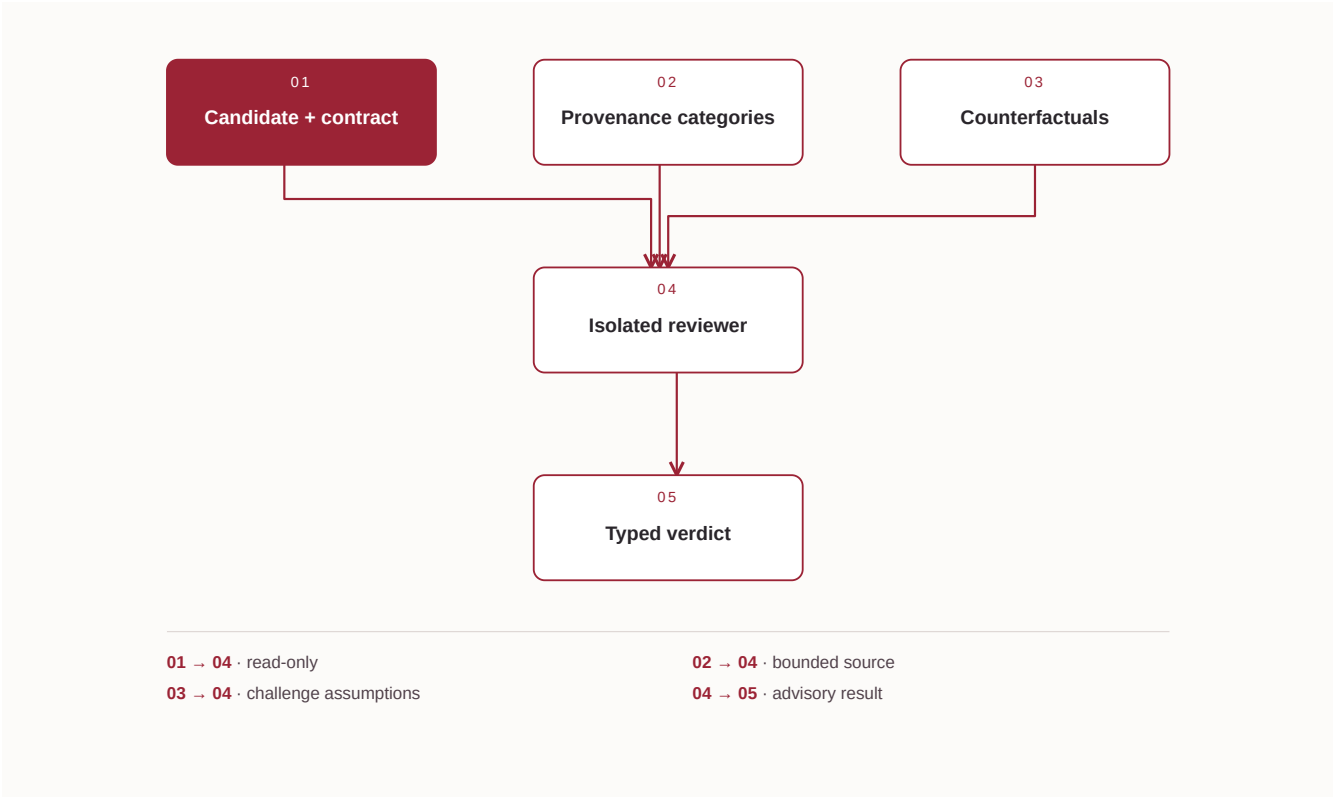
Implemented

Candidate publication

INDEPENDENT CAPABILITY REVIEW

Test what happens when the names change

An isolated reviewer checks a candidate against its contract and provenance. Counterfactual cases change names, ordering, missing evidence and competing candidates to assess whether the behavior generalizes.



Independent capability review · overview.

The reviewer receives a read-only packet and returns a typed verdict. Generation, review and execution permission remain separately owned.

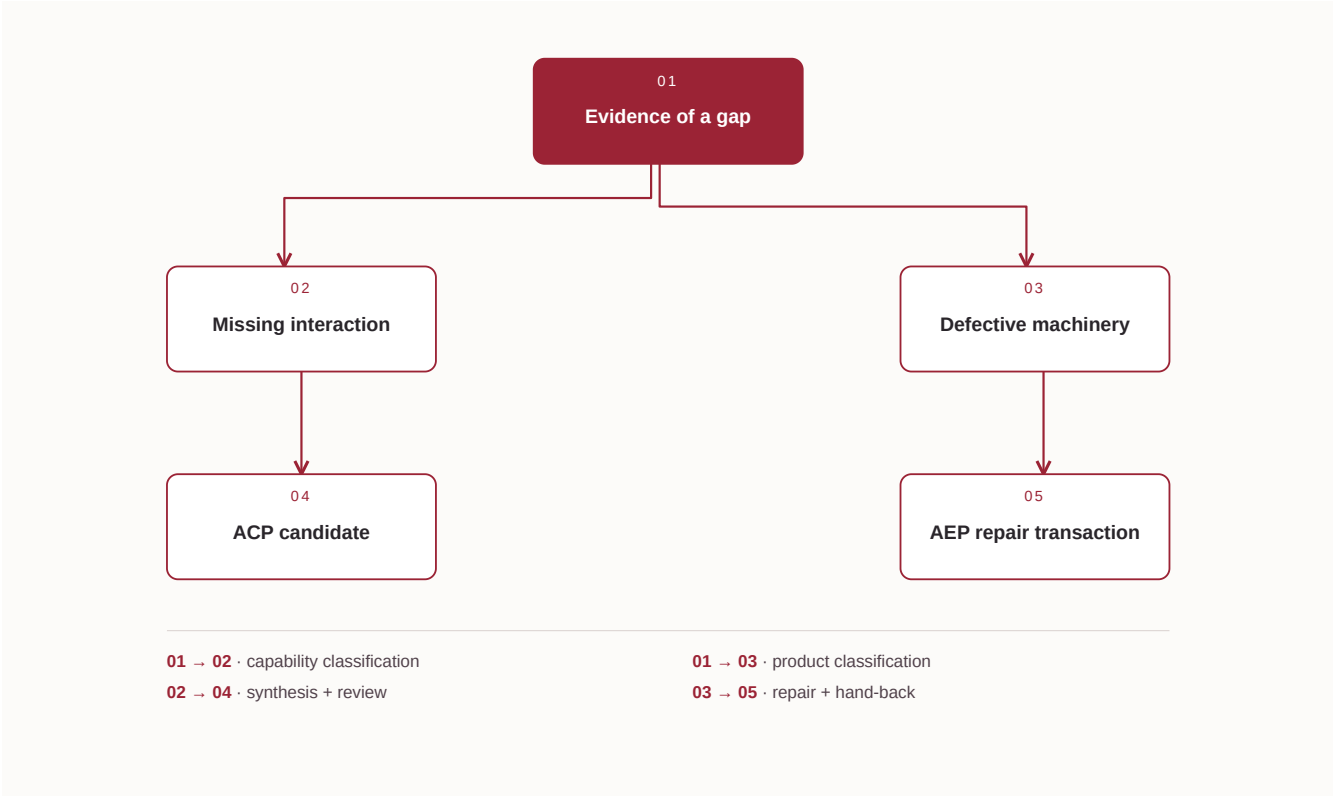
Implemented

Independent capability review

RUNTIME SOFTWARE REPAIR

Repair has to end with a working hand-back

The Autonomic Engineering Plane (AEP) is an adaptive software-repair harness. It owns diagnosis, a persistent repair session, scoped changes, tests, build admission and hot replacement, ending with verified hand-back to the run.



Runtime software repair · overview.

A missing interaction belongs to capability development; a defect in supported platform behavior belongs to software repair. The repair loop is assessed as a complete transaction, beyond the existence of a patch.

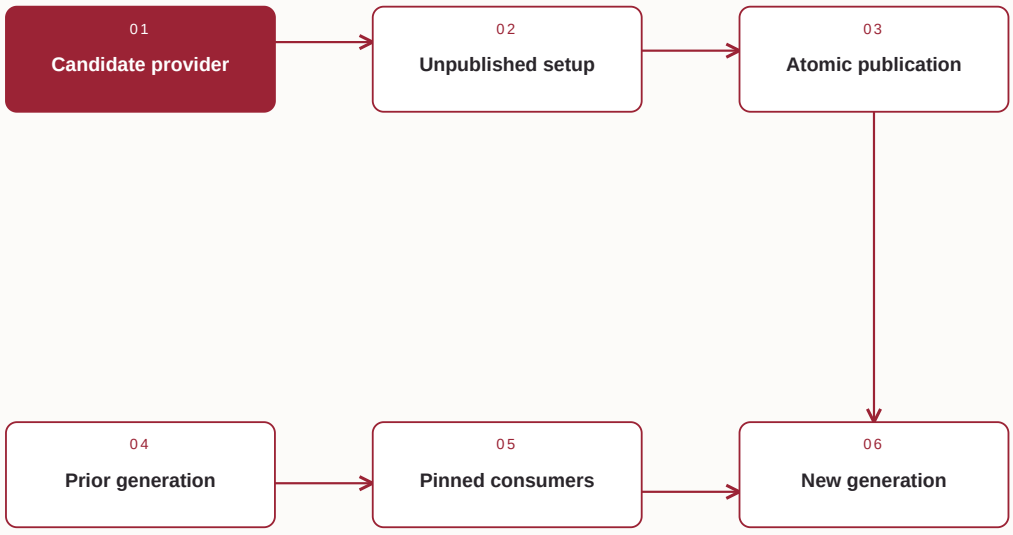
Implemented

Runtime software repair

PROVIDER REPLACEMENT

Replace the worker. Retain the record.

Versioned providers give runtime replacement a defined boundary. New work can adopt a replacement while existing work retains its implementation and the engagement state stays outside the provider.



Provider replacement · overview.

The Runtime Composition Kernel owns publication, leases, rollback and cleanup. This supplies the lifecycle foundation for repair without requiring the investigation record to move with the code.

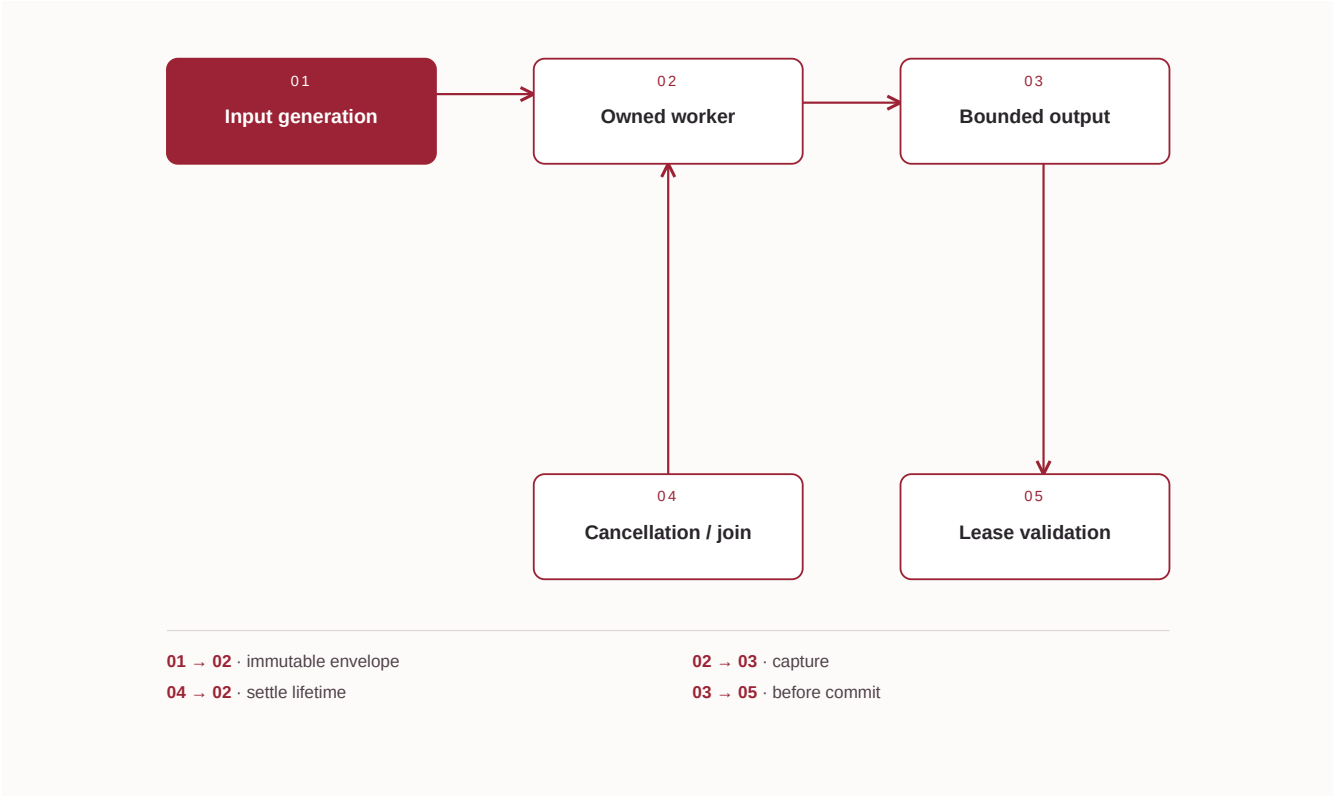
Implemented

Provider replacement

WORKER RESULT ATTRIBUTION

Old work cannot silently become current

Isolated workers receive immutable execution envelopes. Acceptance checks the artifact, input and generation lease, so an expired worker cannot publish a plausible result into the current run.



Worker result attribution · overview.

In-process handlers and isolated workers have different replacement boundaries. A lease identifies the implementation responsible for a result. Process ownership, bounded output, cleanup handles and token accounting make resource use inspectable.

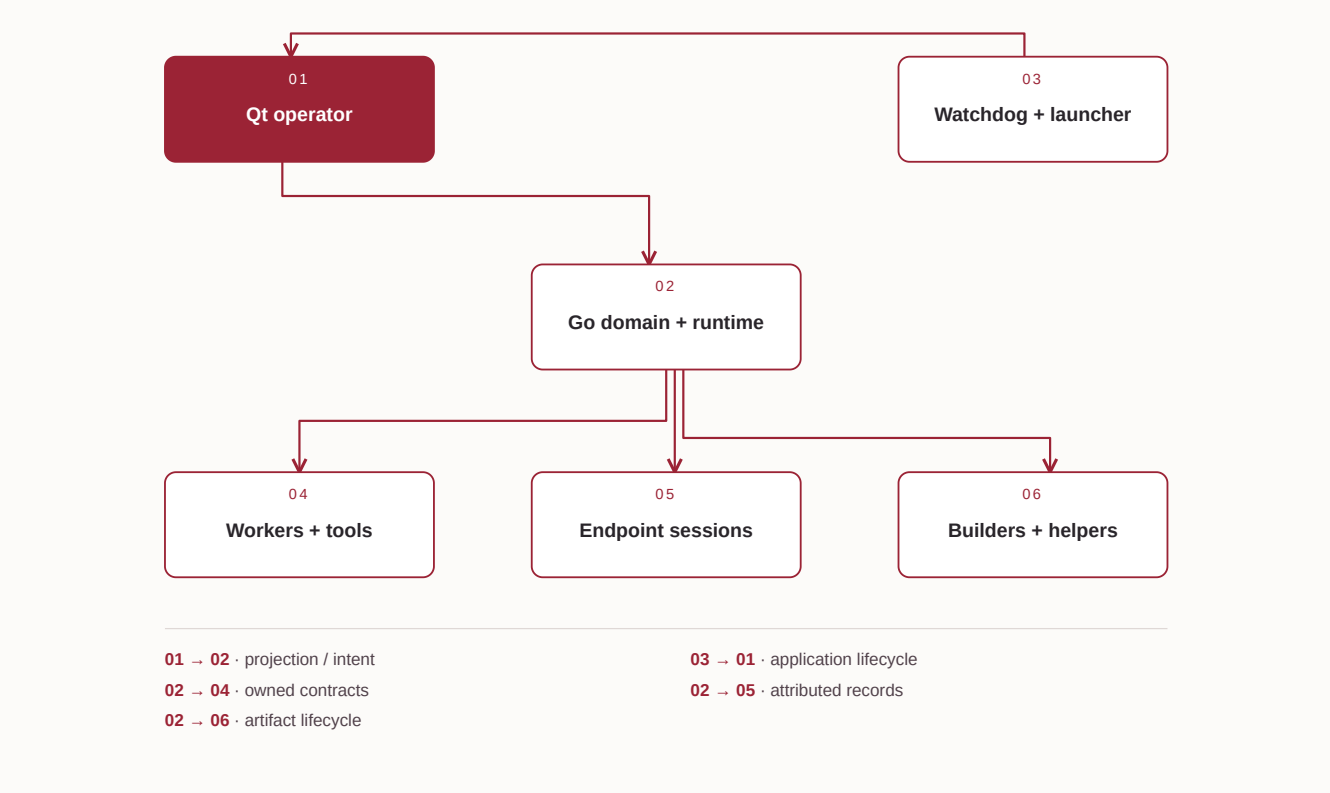
Implemented

Worker result attribution

WORKSPACE INTEGRATION

Keep specialist tools in their native setting

The Qt workspace combines dense investigation views with retained tool surfaces. Gitea, BloodHound, build workflows, RDP and development harnesses can sit alongside the operator environment.



Workspace integration · overview.

Lightweight QML chrome surrounds native widgets. Embedded windows preserve specialist interfaces while the investigation remains visible. Binary and source analysis remain beside the workbench; their results return to the same investigation record.

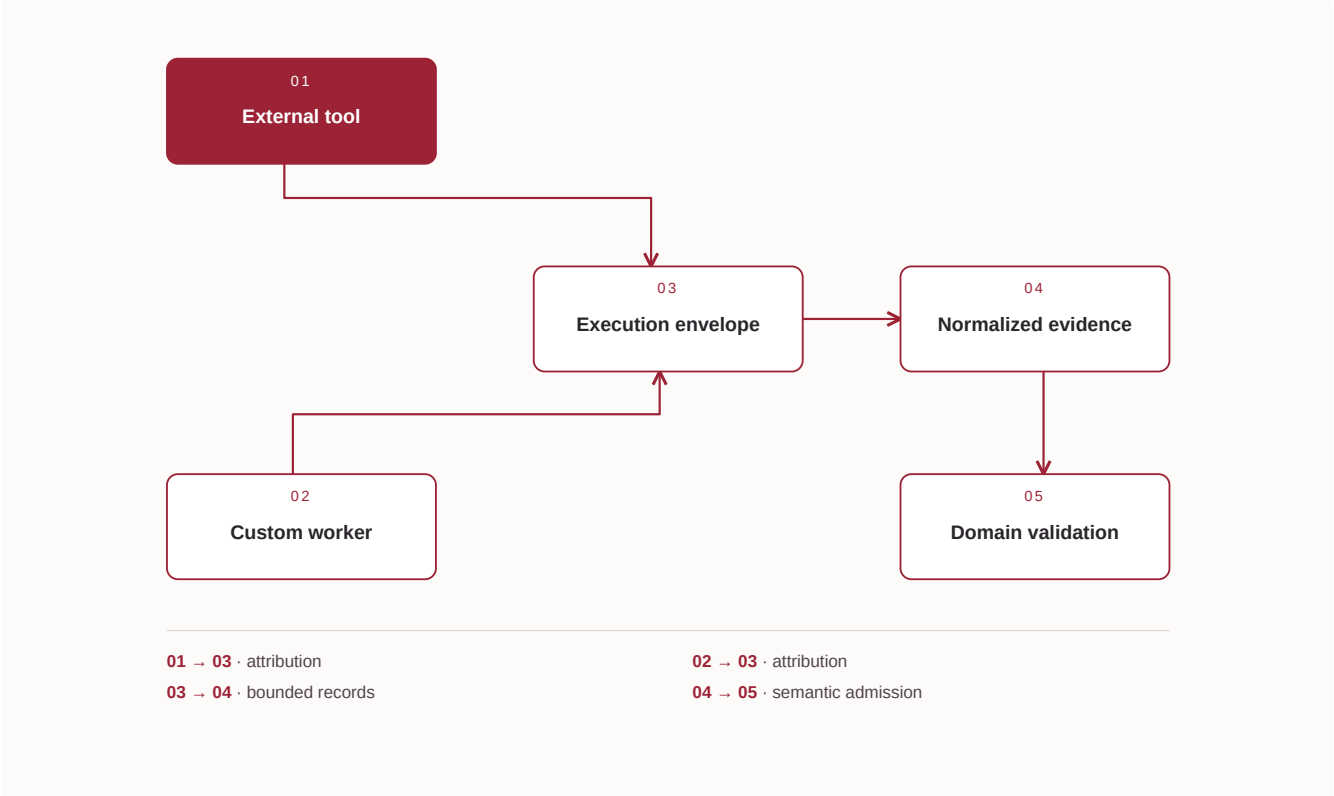
Implemented

Workspace integration

THIRD-PARTY EXECUTION

Integration begins after the tool runs

Network, web, directory, browser and source-inspection tools produce different kinds of output. Their value to the platform comes from controlled execution and the attributed evidence returned to the engagement.



Third-party execution · overview.

Admitted third-party proof-of-concept work can use isolated containers. Tool availability, candidate review and execution permission remain separate inputs.

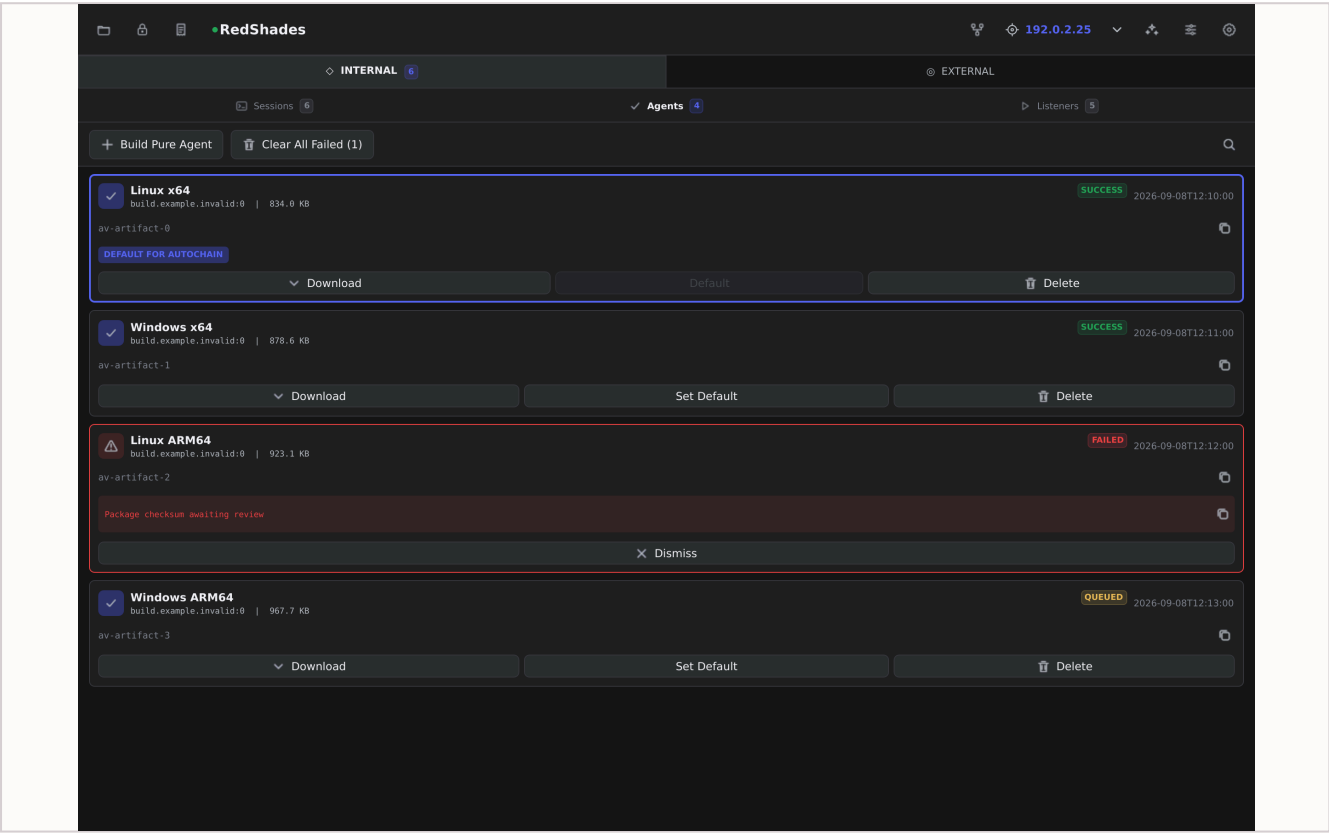
Implemented

Third-party execution

ARTIFACT IDENTITY

Built bytes need a traceable identity

Versioned builds, transformation and obfuscation components form the artifact toolchain. VM-oriented transformation sits within that engineering scope; digests and provenance connect the resulting material to its recorded role.



Compare versioned artifacts and their build states.

Native artifact views expose the inventory to the operator. A build record identifies material and purpose without implying that the artifact was deployed or a session established.

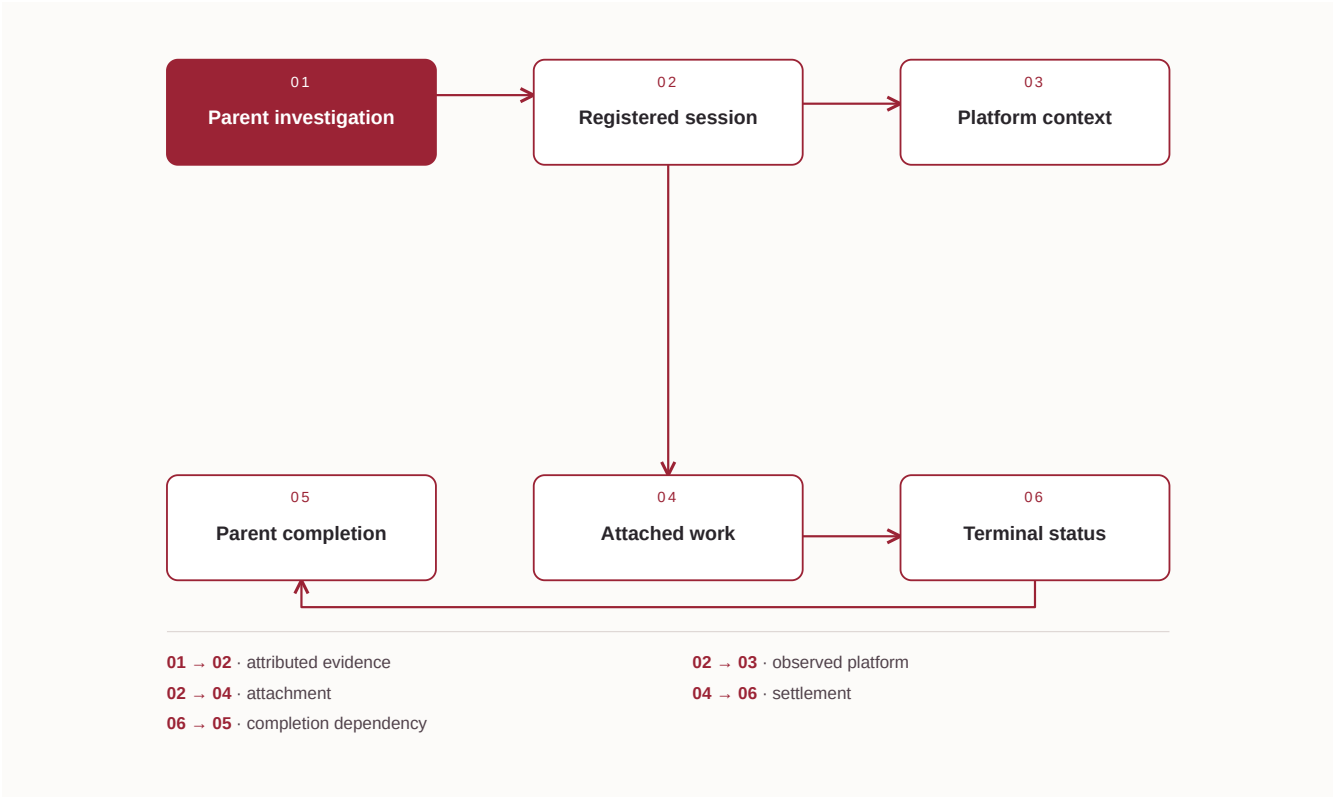
Implemented

Artifact identity

SESSION CONTINUATION

A session adds context to the same investigation

Registered sessions make platform-aware continuation available. Common, Windows and Linux stage families retain their prerequisites while artifacts and attached work remain linked to the parent engagement.



Session continuation · overview.

The 13 C2 continuation declarations complement the 88 Core stages. Session context selects applicable work.

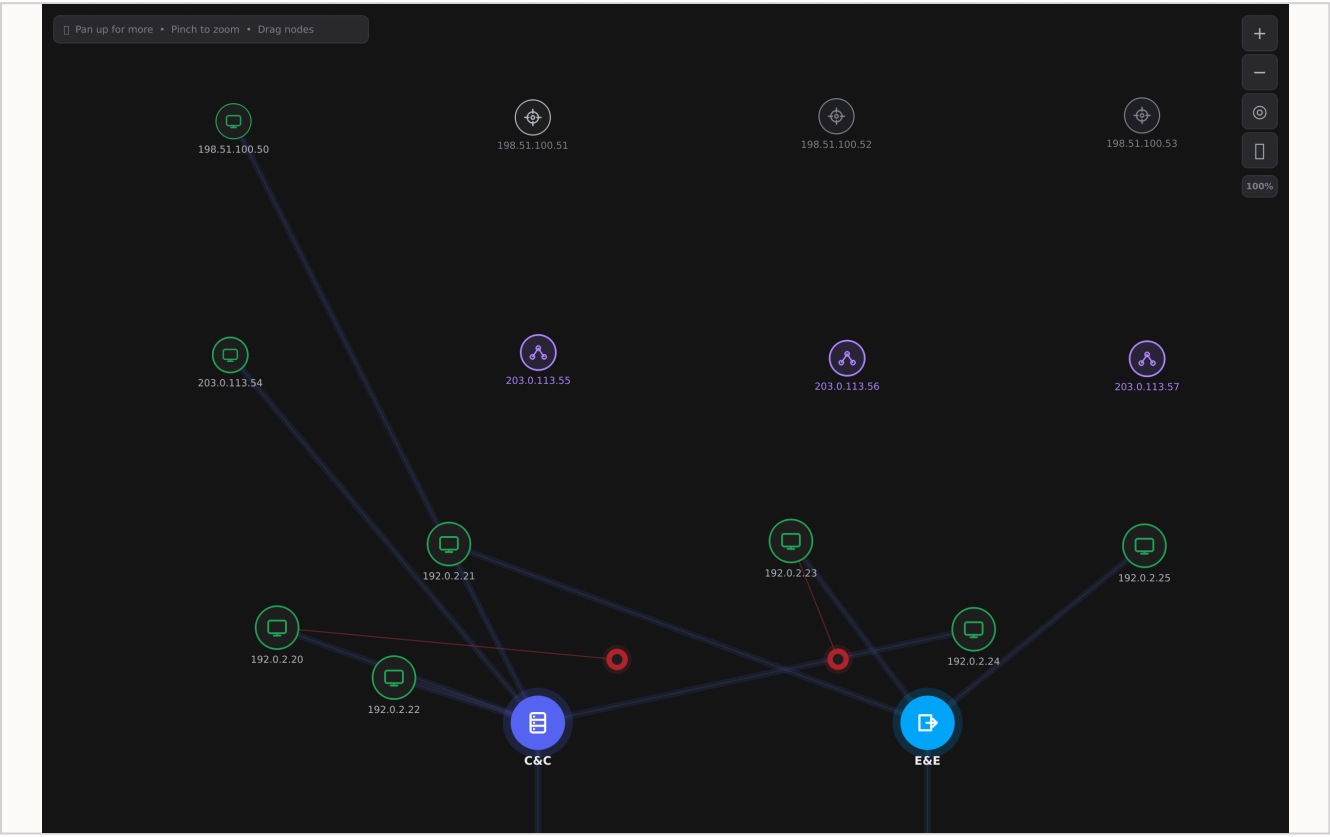
Implemented

Session continuation

NETWORK GRAPH

See where an observation belongs

Network Graph places observed hosts and relationships in the wider investigation. Selecting a host or link connects that overview to its available context.



Locate each host and its observed relationships in the wider investigation.

A displayed relationship aids orientation. Its presence does not establish an admitted route or a verified capability.

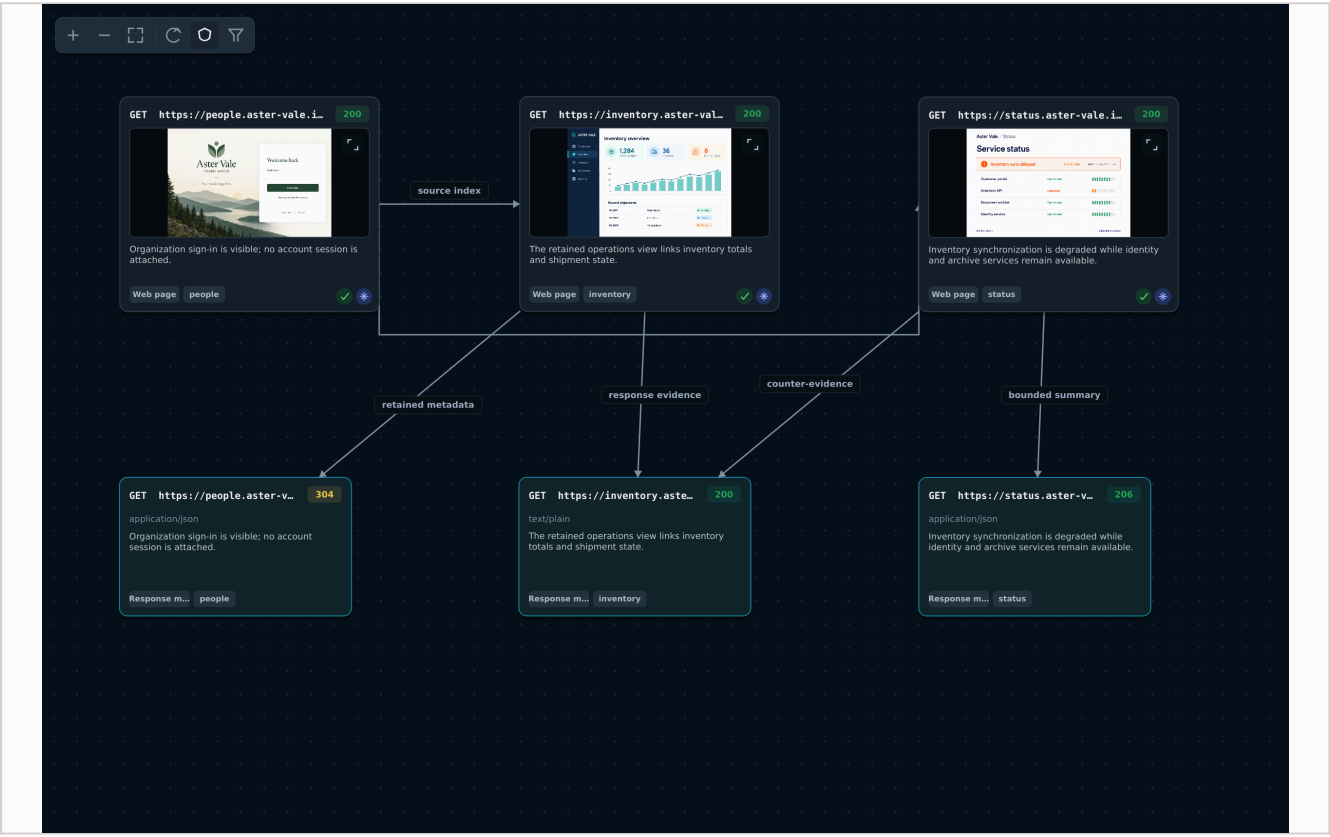
Native interface

Network Graph

WEBRECON OVERVIEW

Read the source without losing the overview

WebRecon places web observations, source detail and endpoint review in one native surface. The operator can inspect a selected item while retaining the surrounding investigation.



Follow web observations from the page to the evidence record.

Source material stays near the observation it supports, with selected evidence and review context available together.

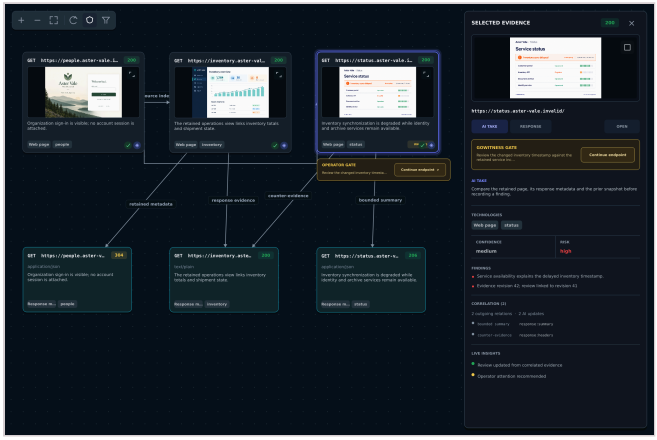
Native interface

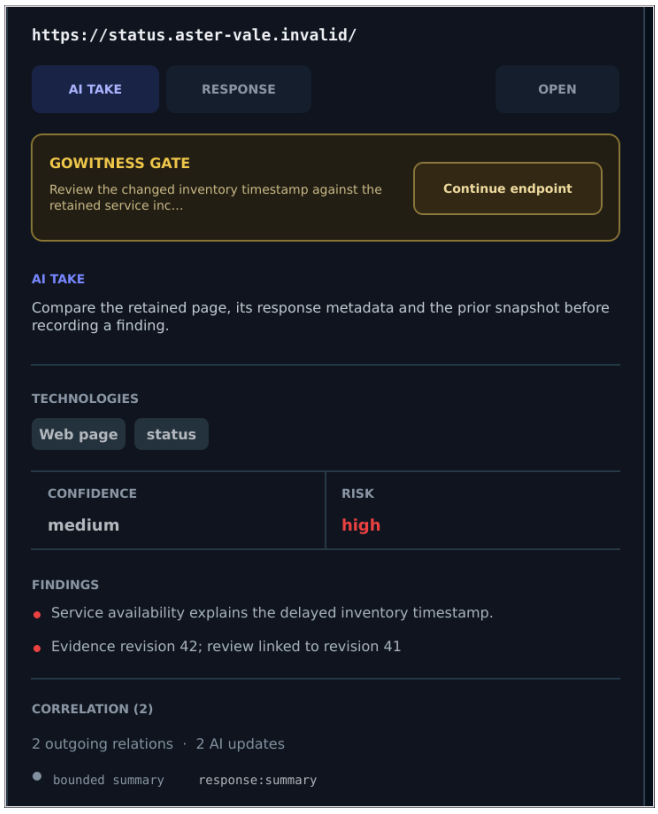
WebRecon overview

WEBRECON REVIEW AND GATE STATE

Make the pending decision specific

A review state identifies the affected endpoint or branch and its supporting evidence. The operator can see what is waiting and where the decision applies.





See the endpoint, scope and evidence behind a pending review.

A displayed gate communicates scope. Enforcement is established by policy and lifecycle validation, beyond the screenshot.

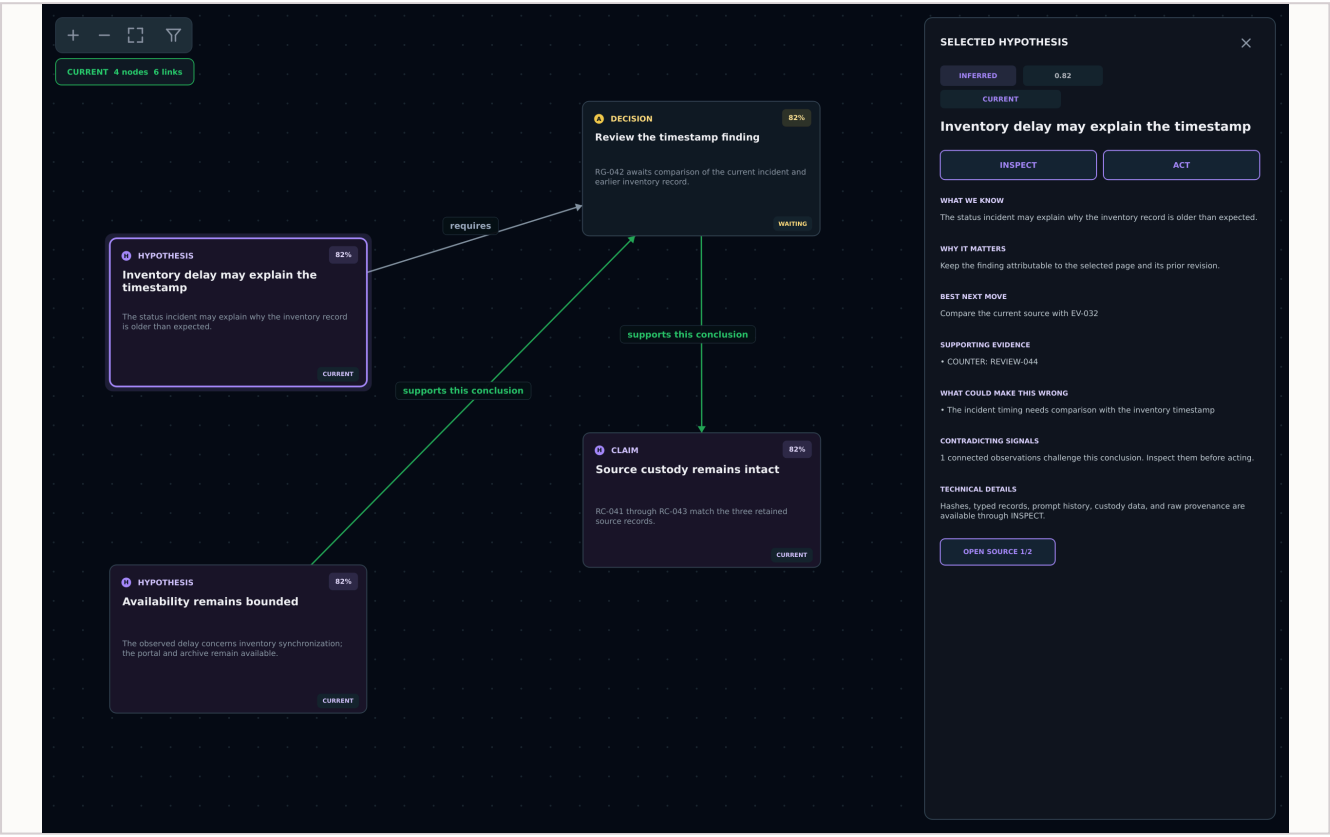
Native interface

WebRecon review and gate state

INVESTIGATION GRAPH

Trace a hypothesis to its observations

Investigation Graph arranges evidence and interpretations as relationships. Detail views retain the source references needed to examine a hypothesis.



Trace each conclusion through support, counter-evidence and review.

The graph offers an overview while the workbench carries fuller records. Observations remain distinct from their interpretation.

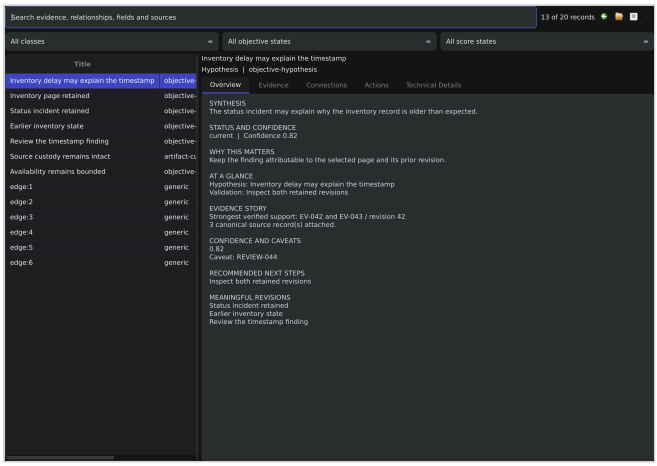
Native interface

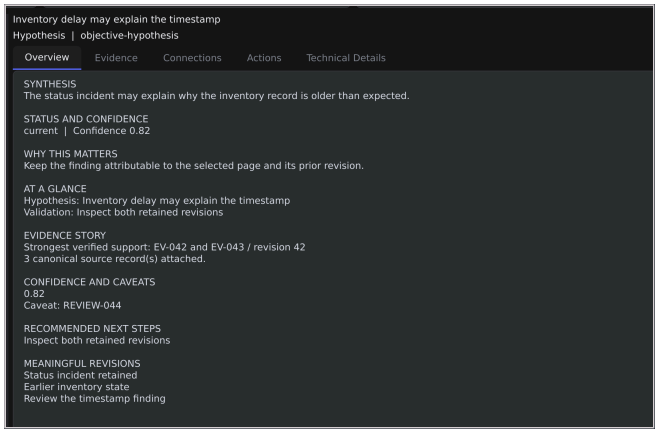
Investigation Graph

INVESTIGATION WORKBENCH

Give difficult evidence room

The Investigation Workbench provides a dedicated surface for source references, context and available continuation. Selection exposes detail without forcing every field into a graph node.





Compare canonical records and the sources behind the current revision.

Review source references, competing observations and the current revision together. Open the image to inspect the record in detail.

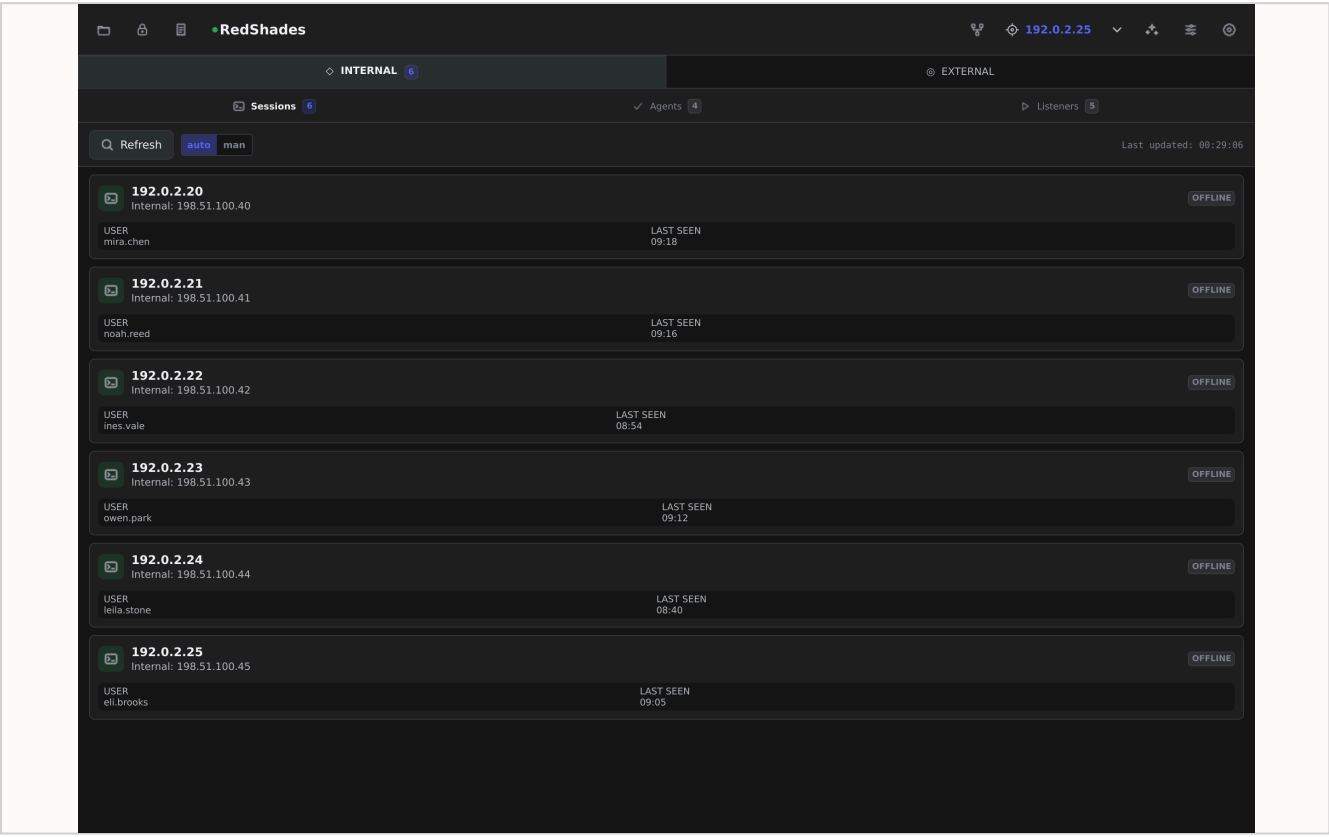
Native interface

Investigation Workbench

SESSION AND ARTIFACT SURFACES

Distinguish a record from availability

Session and artifact views place stored records, versioned builds and observed availability together. Offline and unknown states remain visible alongside selected detail.



Review host identity and recorded availability before continuing work.

Host identity, recorded state and artifact history help an operator distinguish stored records from current availability.

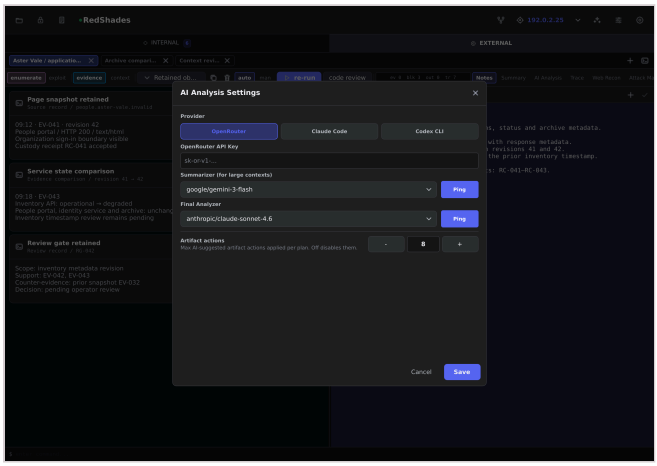
Native interface

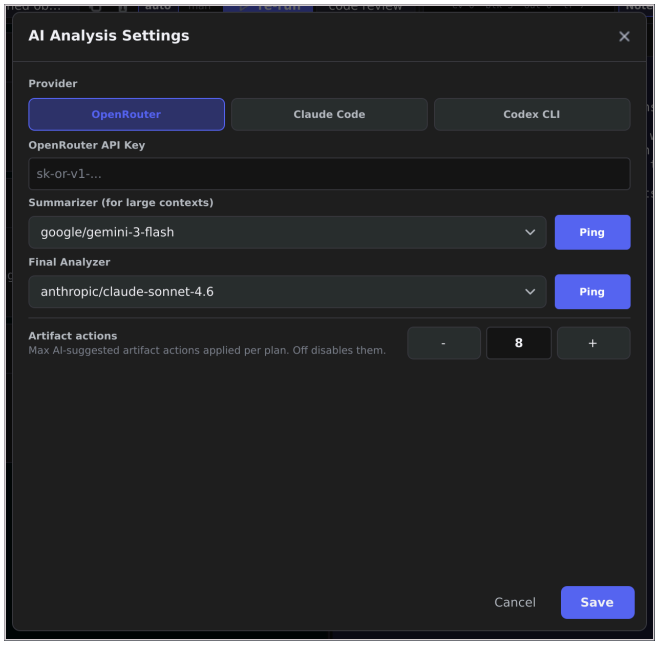
Session and artifact surfaces

MODEL AND RUNTIME CONTROLS

Configuration within reach of the work

Model and runtime controls remain accessible alongside the investigation. They expose the choices an operator needs to review without leaving the native workspace.





Review model selection and bounded provider settings.

Configuration expresses the selected policy. Runtime admission, attribution and accounting establish how that policy is applied.

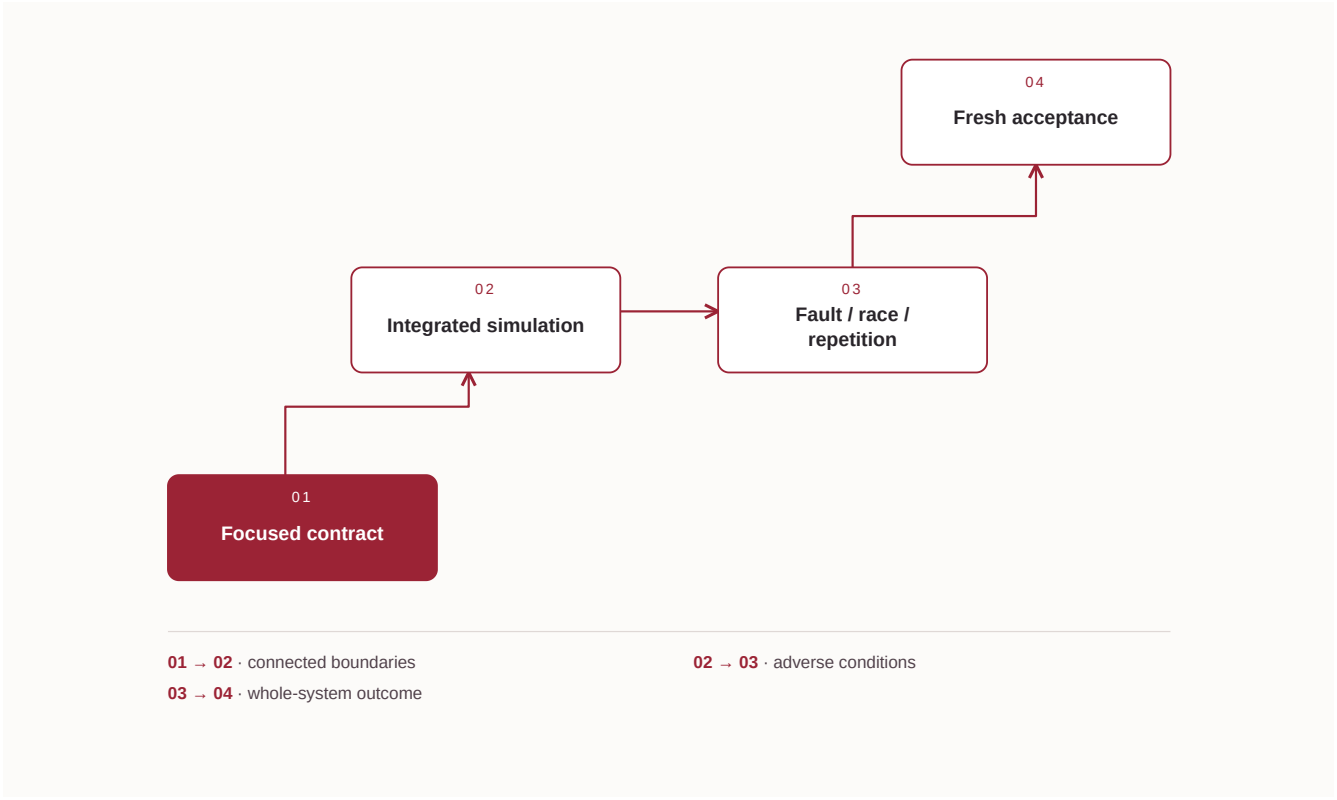
Native interface

Model and runtime controls

VERIFICATION COVERAGE

Match the claim to the check

Focused contracts, integrated simulations, race checks, repetition, fuzzing and fault injection examine different failure modes. The Mega and Ultra acceptance suites organize that work.



Verification coverage · overview.

Revision-bound receipts connect checks to commands and outputs. A component result supports its tested boundary; whole-system reliability needs integrated evidence.

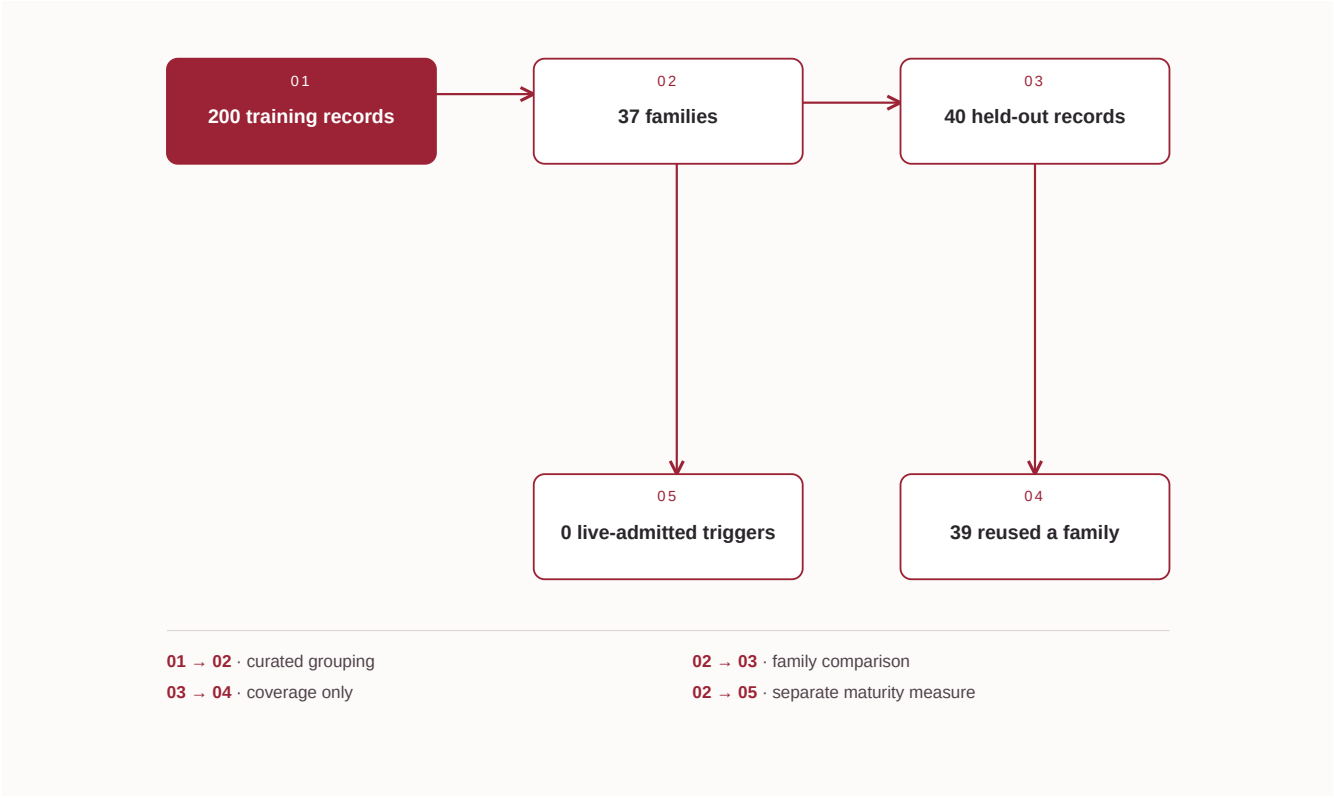
Implemented

Verification coverage

DISCLOSURE STUDY

A vocabulary that can be tested on new material

The Trigger Methodology Graph study grouped 200 public disclosures into 37 recurring families. Of 40 identity-disjoint held-out disclosures, 39 belonged to a represented family.



Disclosure study · overview.

This measures family coverage in a curated study. It does not count discoveries made by the product. Synthetic calibration recorded 600 activations; no candidates were live-exercised or admitted in the reported study.

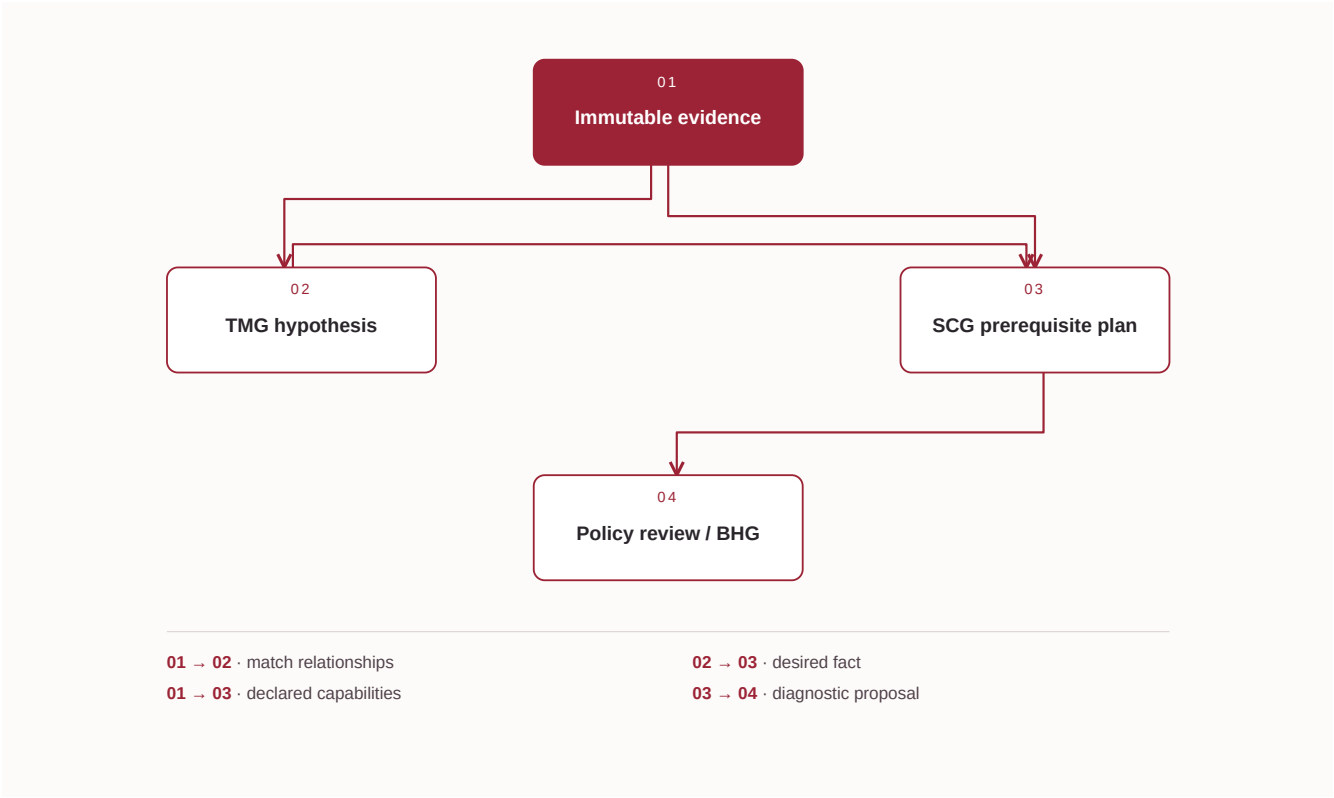
Retained study

Disclosure study

EVIDENCE-GAP ANALYSIS

A useful hypothesis names the missing fact

Trigger Methodology Graph produces evidence-bound hypotheses. Shadow Capability Graph examines missing prerequisites from an immutable snapshot. Policy gates retain review over proposed hypotheses.



Evidence-gap analysis · overview.

The result identifies uncertainty and the evidence needed to resolve it. A diagnostic suggestion does not acquire scheduling authority.

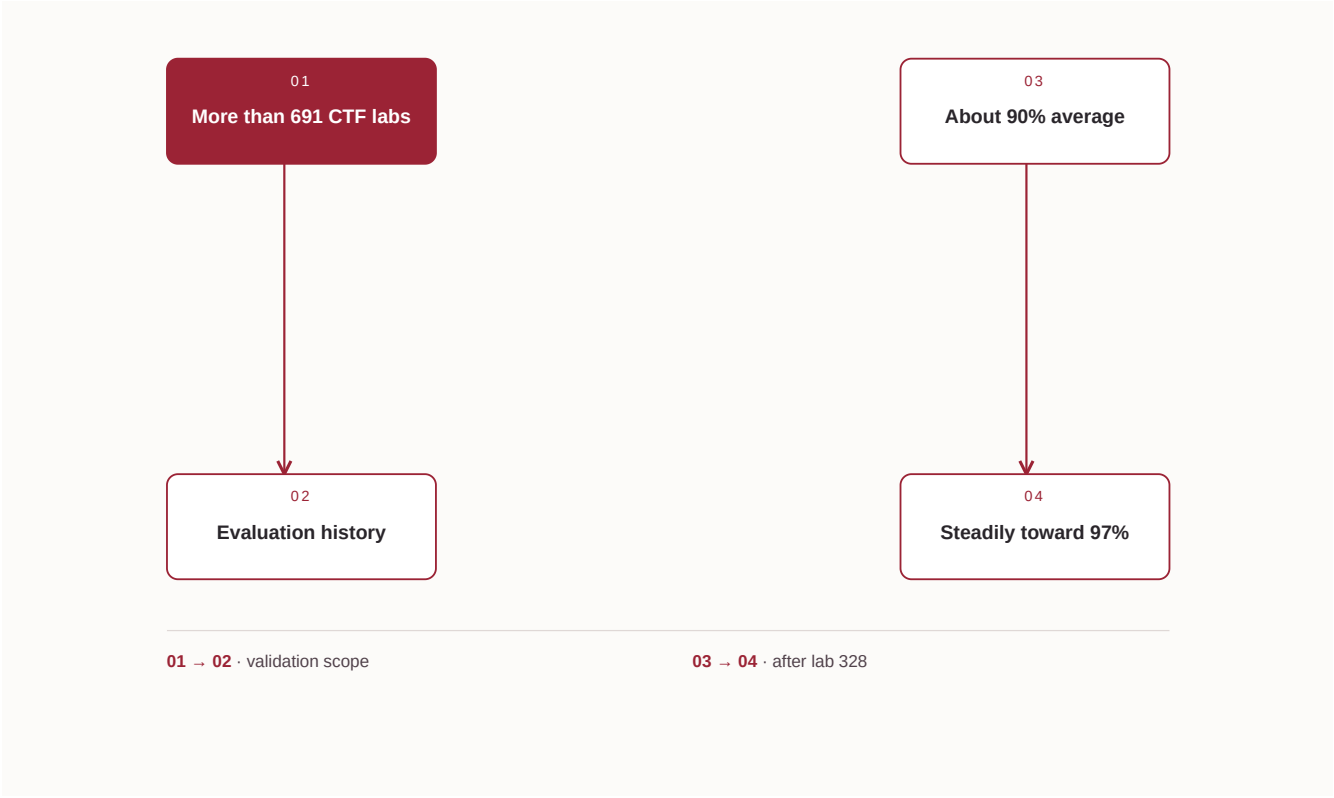
Implemented

Evidence-gap analysis

CTF VALIDATION

An evaluation history across more than 691 CTF labs

Validation spans more than 691 CTF labs. The learning curve averaged about 90% after lab 328 and rose steadily toward 97%.



CTF validation · overview.

Successive evaluations connect model learning with the practical demands of sustained technical work. The history complements the platform's component, integration and fault-testing program.

Evaluation history

CTF validation

88 AUTOMATIC DECLARATIONS · CONDITIONAL GRAPH

Core stage atlas

Each entry identifies available work and its evidence context. Separate C2 families extend session work.

implant deployment Validated Core

`implant_deployment`

Artifact and session work · Admitted artifact and authorized context → Artifact/session records

ACL operator review (post-summary) Validated Core

`acl_operator_action`

Directory analysis · Directory evidence and operator review → Review record

AD compositional capability planning Validated Core

`ad_capability_planning`

Directory analysis · Directory evidence → Directory analysis records

AD effective capability discovery Validated Core

`ad_capability_discovery`

Directory analysis · Directory evidence → Directory analysis records

BloodHound collection Validated Core

`bloodhound_collection`

Directory analysis · Directory context → Graph analysis material

Cross-realm Kerberos service-ticket custody Validated Core

`ad_cross_realm_kerberos`

Directory analysis · Directory evidence → Directory analysis records

masscan discovery Validated Core

`discovery_masscan`

Discovery · Scope and observation context → Network observations

nmap service and OS scan Validated Core

`discovery_nmap`

Discovery · Scope and observation context → Network observations

Results return to the evidence-driven scheduler. Stage declarations describe available work, not a mandatory linear sequence.

Source-derived inventory

88 Core stages

88 AUTOMATIC DECLARATIONS · CONDITIONAL GRAPH

Core stage atlas

Each entry identifies available work and its evidence context. Separate C2 families extend session work.

passive OSINT (WHOIS / DNS / ASN) Validated Core

`osint_passive`

Discovery · Scope and public observations → Context evidence

query discovered ports Validated Core

`discovery_ports`

Discovery · Scope and observation context → Network observations

BloodHound ACL attack path analysis Validated Core

`post_acl_analysis`

Extended investigation · Session, artifact or investigation context → Attributed investigation records

chisel SOCKS5 reverse pivot Validated Core

`post_pivot_chisel`

Extended investigation · Session, artifact or investigation context → Attributed investigation records

DCSync domain hash dump Validated Core

`post_dcsync`

Extended investigation · Session, artifact or investigation context → Attributed investigation records

Disabled legacy advisory handoff Validated Core

`post_nopac`

Extended investigation · Session, artifact or investigation context → Attributed investigation records

DPAPI artifact analysis (operator action) Validated Core

`post_dpapi`

Extended investigation · Session, artifact or investigation context → Attributed investigation records

Final assessment report Validated Core

`post_pwndoc_export`

Extended investigation · Session, artifact or investigation context → Attributed investigation records

Results return to the evidence-driven scheduler. Stage declarations describe available work, not a mandatory linear sequence.

Source-derived inventory

88 Core stages

88 AUTOMATIC DECLARATIONS · CONDITIONAL GRAPH

Core stage atlas

Each entry identifies available work and its evidence context. Separate C2 families extend session work.

Linux privilege escalation enumeration Validated Core

`post_linux_privesc`

Extended investigation · Session, artifact or investigation context → Attributed investigation records

pass-the-hash sweep Validated Core

`post_pth`

Extended investigation · Session, artifact or investigation context → Attributed investigation records

pass-the-ticket (golden/silver ticket) Validated Core

`post_ptt`

Extended investigation · Session, artifact or investigation context → Attributed investigation records

secretsdump credential harvest Validated Core

`post_secretsdump`

Extended investigation · Session, artifact or investigation context → Attributed investigation records

SMB binary credential extraction Validated Core

`post_smb_binary_analysis`

Extended investigation · Session, artifact or investigation context → Attributed investigation records

Windows privilege escalation enumeration Validated Core

`post_windows_privesc`

Extended investigation · Session, artifact or investigation context → Attributed investigation records

AD coercion (PrinterBug/PetitPotam/DFSCoerce) Validated Core

`identity_coerce`

Identity analysis · Identity and service context → Identity evidence

certipy AD CS Validated Core

`identity_certipy`

Identity analysis · Identity and service context → Identity evidence

Results return to the evidence-driven scheduler. Stage declarations describe available work, not a mandatory linear sequence.

Source-derived inventory

88 Core stages

88 AUTOMATIC DECLARATIONS · CONDITIONAL GRAPH

Core stage atlas

Each entry identifies available work and its evidence context. Separate C2 families extend session work.

certipy AD CS exploitation (ESC1/ESC4/ESC8) Validated Core

`identity_certipy_exploit`

Identity analysis · Identity and service context → Identity evidence

enum4linux-ng Validated Core

`identity_enum4linux`

Identity analysis · Identity and service context → Identity evidence

GetNPUsers Validated Core

`identity_getnpusers`

Identity analysis · Identity and service context → Identity evidence

GetUserSPNs Validated Core

`identity_getuserspns`

Identity analysis · Identity and service context → Identity evidence

hash cracking Validated Core

`identity_hash_cracking`

Identity analysis · Identity and service context → Identity evidence

kerbrute Validated Core

`identity_kerbrute`

Identity analysis · Identity and service context → Identity evidence

LAPS password dump Validated Core

`identity_laps`

Identity analysis · Identity and service context → Identity evidence

ldapdomaindump Validated Core

`identity_ldapdomaindump`

Identity analysis · Identity and service context → Identity evidence

Results return to the evidence-driven scheduler. Stage declarations describe available work, not a mandatory linear sequence.

Source-derived inventory

88 Core stages

88 AUTOMATIC DECLARATIONS · CONDITIONAL GRAPH

Core stage atlas

Each entry identifies available work and its evidence context. Separate C2 families extend session work.

lookupsid Validated Core

`identity_lookupsid`

Identity analysis · Identity and service context → Identity evidence

NTLM relay (ntlmrelayx) Validated Core

`identity_ntlm_relay`

Identity analysis · Identity and service context → Identity evidence

nxc null/guest enumeration Validated Core

`identity_nxc_guest`

Identity analysis · Identity and service context → Identity evidence

Responder NTLM hash capture Validated Core

`identity_ntlm_capture`

Identity analysis · Identity and service context → Identity evidence

targeted credential spray Validated Core

`identity_credential_spray`

Identity analysis · Identity and service context → Identity evidence

username permutation generation Validated Core

`identity_username_anarchy`

Identity analysis · Identity and service context → Identity evidence

credential reuse sweep Validated Core

`credential_reuse_sweep`

Investigation · Scoped evidence → Attributed records

Execution context: network path and domain time Validated Core

`environment_adaptation`

Platform adaptation · Environment context → Adaptation records

Results return to the evidence-driven scheduler. Stage declarations describe available work, not a mandatory linear sequence.

Source-derived inventory

88 Core stages

88 AUTOMATIC DECLARATIONS · CONDITIONAL GRAPH

Core stage atlas

Each entry identifies available work and its evidence context. Separate C2 families extend session work.

conditional mssqlclient Validated Core

`remote_mssqlclient`

Remote services · Service and authorized session context → Protocol evidence

conditional smbclient Validated Core

`remote_smbclient`

Remote services · Service and authorized session context → Protocol evidence

Kerberos ticket-backed WinRM validation Validated Core

`remote_kerberos_winrm`

Remote services · Service and authorized session context → Protocol evidence

MSSQL linked server ADIDNS poisoning Validated Core

`mssql_linked_server_poison`

Remote services · Database context → Database evidence

SMB file harvest Validated Core

`remote_smb_harvest`

Remote services · Service and authorized session context → Protocol evidence

smbmap share enumeration Validated Core

`remote_smbmap`

Remote services · Service and authorized session context → Protocol evidence

deterministic operator report Validated Core

`summary`

Reporting · Retained investigation evidence → Report projection

DNS zone transfer drill Validated Core

`service_dns_axfr`

Service analysis · Service observations → Service evidence

Results return to the evidence-driven scheduler. Stage declarations describe available work, not a mandatory linear sequence.

Source-derived inventory

88 Core stages

88 AUTOMATIC DECLARATIONS · CONDITIONAL GRAPH

Core stage atlas

Each entry identifies available work and its evidence context. Separate C2 families extend session work.

dnsx Validated Core

`service_dnsx`

Service analysis · Service observations → Service evidence

FTP anonymous Validated Core

`service_ftp_anon`

Service analysis · Service observations → Service evidence

IPMI enumeration and hash extraction Validated Core

`service_ipmi`

Service analysis · Service observations → Service evidence

MySQL probe Validated Core

`service_mysql`

Service analysis · Service observations → Service evidence

NFS enumeration Validated Core

`service_nfs`

Service analysis · Service observations → Service evidence

Redis enumeration Validated Core

`service_redis`

Service analysis · Service observations → Service evidence

service CVE candidate sweep Validated Core

`service_searchsploit_sweep`

Service analysis · Service observations → Service evidence

service CVE workbench Validated Core

`service_cve_workbench`

Service analysis · Service observations → Service evidence

Results return to the evidence-driven scheduler. Stage declarations describe available work, not a mandatory linear sequence.

Source-derived inventory

88 Core stages

88 AUTOMATIC DECLARATIONS · CONDITIONAL GRAPH

Core stage atlas

Each entry identifies available work and its evidence context. Separate C2 families extend session work.

SMTP user enumeration Validated Core

`service_smtp_user_enum`

Service analysis · Service observations → Service evidence

SNMP enumeration Validated Core

`service_snmp_enum`

Service analysis · Service observations → Service evidence

ssh-audit Validated Core

`service_ssh_audit`

Service analysis · Service observations → Service evidence

subfinder Validated Core

`service_subfinder`

Service analysis · Service observations → Service evidence

credential to shell attempts Validated Core

`shell_attempts`

Session work · Authorized execution context → Session-related records

xfreerdp RDP session Validated Core

`rdp_session`

Session work · Authorized session context → Session records

CMS scanning Validated Core

`web_cms_scan`

Web investigation · Web observations and scoped review → Web evidence

CMS/app-server RCE (Tomcat/Jenkins/Drupal) Validated Core

`web_cms_exploit`

Web investigation · Web observations and scoped review → Web evidence

Results return to the evidence-driven scheduler. Stage declarations describe available work, not a mandatory linear sequence.

Source-derived inventory

88 Core stages

88 AUTOMATIC DECLARATIONS · CONDITIONAL GRAPH

Core stage atlas

Each entry identifies available work and its evidence context. Separate C2 families extend session work.

CVE PoC workbench review Validated Core

`web_cve_poc_workbench`

Web investigation · Web observations and scoped review → Web evidence

GoWitness endpoint review Validated Core

`web_screenshot`

Web investigation · Web observations and scoped review → Web evidence

HTTP verb tampering Validated Core

`web_verb_tampering`

Web investigation · Web observations and scoped review → Web evidence

IDOR / parameter enumeration Validated Core

`web_idor_probe`

Web investigation · Web observations and scoped review → Web evidence

LFI exploitation Validated Core

`web_lfi_exploit`

Web investigation · Web observations and scoped review → Web evidence

nuclei parallel Validated Core

`web_nuclei`

Web investigation · Web observations and scoped review → Web evidence

OS command injection probe Validated Core

`web_cmdi_probe`

Web investigation · Web observations and scoped review → Web evidence

post-auth CVE PoC workbench review Validated Core

`web_post_auth_poc_workbench`

Web investigation · Web observations and scoped review → Web evidence

Results return to the evidence-driven scheduler. Stage declarations describe available work, not a mandatory linear sequence.

Source-derived inventory

88 Core stages

88 AUTOMATIC DECLARATIONS · CONDITIONAL GRAPH

Core stage atlas

Each entry identifies available work and its evidence context. Separate C2 families extend session work.

post-auth exploit probes Validated Core

`web_post_auth_exploit_probes`

Web investigation · Web observations and scoped review → Web evidence

post-auth surface harvest Validated Core

`web_post_auth_harvest`

Web investigation · Web observations and scoped review → Web evidence

SQLi OS shell (--os-cmd / --os-shell) Validated Core

`web_sqli_post_exploit`

Web investigation · Web observations and scoped review → Web evidence

SQLi probe Validated Core

`web_sqli_probe`

Web investigation · Web observations and scoped review → Web evidence

SSTI probe Validated Core

`web_ssti_probe`

Web investigation · Web observations and scoped review → Web evidence

target-specific password generation Validated Core

`web_cewl`

Web investigation · Web observations and scoped review → Web evidence

web content analysis Validated Core

`web_content_analysis`

Web investigation · Web observations and scoped review → Web evidence

web file upload attack Validated Core

`web_file_upload_attack`

Web investigation · Web observations and scoped review → Web evidence

Results return to the evidence-driven scheduler. Stage declarations describe available work, not a mandatory linear sequence.

Source-derived inventory

88 Core stages

88 AUTOMATIC DECLARATIONS · CONDITIONAL GRAPH

Core stage atlas

Each entry identifies available work and its evidence context. Separate C2 families extend session work.

web fingerprint + wafw00f Validated Core

`web_whatweb_waf`

Web investigation · Web observations and scoped review → Web evidence

web fuzzing (vhost+dir+ext) Validated Core

`web_fuzz`

Web investigation · Web observations and scoped review → Web evidence

web login brute force Validated Core

`web_login_bruteforce`

Web investigation · Web observations and scoped review → Web evidence

web RCE candidate correlation Validated Core

`web_rce_candidate_correlation`

Web investigation · Web observations and scoped review → Web evidence

web RCE confirmation Validated Core

`web_rce_confirm`

Web investigation · Web observations and scoped review → Web evidence

web RCE deployment preparation Validated Core

`web_rce_deployment_prepare`

Web investigation · Web observations and scoped review → Web evidence

XSS probe Validated Core

`web_xss_probe`

Web investigation · Web observations and scoped review → Web evidence

XXE probe Validated Core

`web_xxe_probe`

Web investigation · Web observations and scoped review → Web evidence

Results return to the evidence-driven scheduler. Stage declarations describe available work, not a mandatory linear sequence.

Source-derived inventory

88 Core stages

13 CONTINUATION STAGES

Session work follows platform-specific branches

Registered session context selects Windows, Linux and shared continuation work. These 13 stages complement the 88-stage Validated Core and are included in the 198-stage catalog.

permission enumeration
windows
`windows_permission_enum`

Linux permission enumeration
linux
`linux_permission_enum`

pivot tunnel + internal discovery
Cross-platform
`pivot_tunnel`

filesystem enumeration
windows
`windows_filesystem_enum`

expanded privilege escalation enumeration
windows
`windows_privilege_escalation`

privilege escalation exploitation
windows
`windows_privilege_escalation_exploit`

Windows lateral movement
windows
`windows_lateral_movement`

Windows persistence
windows
`windows_persistence`

Linux filesystem enumeration
linux
`linux_filesystem_enum`

expanded Linux privilege escalation enumeration
linux
`linux_privilege_escalation`

Linux privilege escalation exploitation
linux
`linux_privilege_escalation_exploit`

Linux lateral movement
linux
`linux_lateral_movement`

Linux persistence
linux
`linux_persistence`

88 Core + 13 C2 continuation + 80 Advanced + 17 Ultimate = 198 stages.

C2 continuation

PLANNED INTEGRATIONS · PACKAGING PENDING

Specialist domain and tool relationships

48 descriptors: 37 potential third-party packages, one external Apple toolchain and ten native or custom components. Domain totals overlap through reuse.

Cluster → capability → shared tool architecture

Domain cluster	Analysis capabilities	Primary and alternative components
Android / mobile 8 stages · 10 referenced entries	artifact intake · provenance custody · configuration review · static analysis · topology modeling · evidence correlation · emulation simulation · reporting	Androguard · Apktool · Android bundletool · Cosign · JADX · Mobile Security Framework · RedShades artifact intake · RedShades typed evidence graph · RedShades policy and effect gate · RedShades evidence-backed reporting
Apple platforms 8 stages · 8 referenced entries	artifact intake · provenance custody · binary decomposition · configuration review · static analysis · topology modeling · emulation simulation · reporting	ipsw · LLVM binary utilities · RedShades artifact intake · RedShades typed evidence graph · RedShades policy and effect gate · RedShades privacy/data-flow model · RedShades evidence-backed reporting · Apple codesign/security toolchain
Blockchain 8 stages · 8 referenced entries	artifact intake · provenance custody · static analysis · evidence correlation · emulation simulation · topology modeling · reporting	Cosign · Echidna · Foundry · RedShades artifact intake · RedShades typed evidence graph · RedShades evidence-backed reporting · Slither · Solidity compiler
Bluetooth / BLE / NFC 7 stages · 8 referenced entries	artifact intake · passive capture parsing · configuration review · evidence correlation · topology modeling · reporting	BlueZ btmon · libnfc utilities · RedShades artifact intake · RedShades typed evidence graph · RedShades protocol observation normalizer · RedShades evidence-backed reporting · Wireshark/TShark · Zeek
Wi-Fi / RF 8 stages · 9 referenced entries	artifact intake · topology modeling · passive capture parsing · static analysis · evidence correlation · policy gating · reporting	GNU Radio · RedShades artifact intake · RedShades typed evidence graph · RedShades policy and effect gate · RedShades protocol observation normalizer · RedShades evidence-backed reporting · Suricata · Wireshark/TShark · Zeek
LLM / AI systems 8 stages · 10 referenced entries	artifact intake · topology modeling · configuration review · emulation simulation · evidence correlation · supply chain analysis · reporting	garak · Inspect AI · OSV-Scanner · RedShades artifact intake · RedShades typed evidence graph · RedShades policy and effect gate · RedShades privacy/data-flow model · RedShades evidence-backed reporting · Syft · Trivy

97 expansion stages: 80 Advanced (78 domain stages and two shared helpers) and 17 Ultimate. Licensing and validation apply to each integration. The 48 entries include 47 stage-referenced components and one foundational router.

Under testing / Under development

22 open-source integration candidates · 15 license-review candidates · 5 built-in · 5 custom planned · 1 external

PLANNED INTEGRATIONS · PACKAGING PENDING

Specialist domain and tool relationships

48 descriptors: 37 potential third-party packages, one external Apple toolchain and ten native or custom components. Domain totals overlap through reuse.

Cluster → capability → shared tool architecture

Domain cluster	Analysis capabilities	Primary and alternative components
Satellite / space 7 stages · 10 referenced entries	artifact intake · passive capture parsing · configuration review · topology modeling · emulation simulation · reporting	GNU Radio · gr-satellites · Orekit · RedShades artifact intake · RedShades typed evidence graph · RedShades protocol observation normalizer · RedShades evidence-backed reporting · RedShades OT/space safety model · Wireshark/TShark · Zeek
Quantum readiness 6 stages · 6 referenced entries	cryptographic inventory · evidence correlation · configuration review · topology modeling · emulation simulation · reporting	Cirq · Qiskit SDK · RedShades artifact intake · RedShades cryptographic evidence normalizer · RedShades typed evidence graph · RedShades evidence-backed reporting
Hardware / firmware 9 stages · 11 referenced entries	artifact intake · binary decomposition · supply chain analysis · static analysis · configuration review · evidence correlation · emulation simulation · reporting	Binwalk · Cosign · Ghidra · ipsw · LLVM binary utilities · QEMU · RedShades artifact intake · RedShades typed evidence graph · RedShades evidence-backed reporting · Syft · Trivy
ICS / SCADA 9 stages · 11 referenced entries	artifact intake · passive capture parsing · topology modeling · safety modeling · configuration review · static analysis · evidence correlation · emulation simulation · policy gating	OpenSCAP · QEMU · RedShades artifact intake · RedShades typed evidence graph · RedShades policy and effect gate · RedShades protocol observation normalizer · RedShades evidence-backed reporting · RedShades OT/space safety model · Suricata · Wireshark/TShark · Zeek
Defensive patching 8 stages · 9 referenced entries	supply chain analysis · evidence correlation · static analysis · reporting · policy gating	Cosign · Grype · OSV-Scanner · RedShades typed evidence graph · RedShades defensive change planner · RedShades policy and effect gate · RedShades evidence-backed reporting · Syft · Trivy
Digital forensics 9 stages · 12 referenced entries	provenance custody · artifact intake · forensic analysis · evidence correlation · reporting	Cosign · Plaso · RedShades artifact intake · RedShades typed evidence graph · RedShades policy and effect gate · RedShades evidence-backed reporting · The Sleuth Kit · Velociraptor · Volatility 3 · Wireshark/TShark · YARA · Zeek
Shared Advanced helpers 2 stages · 3 referenced entries	evidence correlation	RedShades artifact intake · RedShades typed evidence graph · RedShades evidence-backed reporting

The two shared helpers normalize cross-domain evidence and correlate observations into a converged assessment record.

97 expansion stages: 80 Advanced (78 domain stages and two shared helpers) and 17 Ultimate. Licensing and validation apply to each integration. The 48 entries include 47 stage-referenced components and one foundational router.

Under testing / Under development

22 open-source integration candidates · 15 license-review candidates · 5 built-in · 5 custom planned · 1 external

UNDER TESTING

Specialist application domains

Android / mobile

8 stages

Under testing

Package metadata, permissions and storage observations give application review a concrete starting point. Device and transport evidence determine the applicable analysis.

Assessment scope
Mobile configuration, application metadata and transport review

Shared tool architecture
10 referenced entries · Androguard, Apktool, Android bundletool, Cosign, JADX, Mobile Security Framework. Native evidence and reporting components complete the cluster.

Apple platforms

8 stages

Under testing

Signing and entitlements connect application behavior to platform permissions. iOS, iPhone and macOS evidence also supports privacy and configuration review.

Assessment scope
Signing, entitlements, privacy settings and platform configuration

Shared tool architecture
8 referenced entries · ipsw, LLVM binary utilities, Apple codesign/security toolchain. Native evidence and reporting components complete the cluster.

Blockchain

8 stages

Under testing

Contract and transaction records support access-control, dependency and governance review. Provenance keeps each conclusion connected to the relevant artifact.

Assessment scope
Contract metadata, access controls and transaction provenance

Shared tool architecture
8 referenced entries · Cosign, Echidna, Foundry, Slither, Solidity compiler. Native evidence and reporting components complete the cluster.

88 Core + 13 C2 continuation + 80 Advanced + 17 Ultimate = 198 stages.

Under testing

UNDER TESTING

Wireless and AI assessment domains

Proximity / BLE / NFC

7 stages

Under testing

Captured advertisements, pairing observations and NFC records preserve the distinctions between protocols and device classes.

Assessment scope
Advertisement, pairing and NFC record analysis

Shared tool architecture
8 referenced entries · BlueZ btmon, libnfc utilities, Wireshark/TShark, Zeek. Native evidence and reporting components complete the cluster.

Wi-Fi / RF

8 stages

Under testing

Recorded traffic and wireless configuration support network, radio and authentication review. Spectrum records add context where the evidence provides it.

Assessment scope
Wireless posture, spectrum records and authentication configuration

Shared tool architecture
9 referenced entries · GNU Radio, Suricata, Wireshark/TShark, Zeek. Native evidence and reporting components complete the cluster.

LLM / AI systems

8 stages

Under testing

Evaluation artifacts connect model behavior to application permissions and data handling. Model, data and application boundaries receive separate attention.

Assessment scope
Evaluation artifacts, data handling and permission boundaries

Shared tool architecture
10 referenced entries · garak, Inspect AI, OSV-Scanner, Syft, Trivy. Native evidence and reporting components complete the cluster.

88 Core + 13 C2 continuation + 80 Advanced + 17 Ultimate = 198 stages.

Under testing

UNDER TESTING

Satellite systems and quantum readiness

Satellite / space

7 stages

Under testing

Ground-system configuration and telemetry artifacts frame the assessment. Ground, link and telemetry evidence retain their different trust boundaries.

Assessment scope
Telemetry formats, asset configuration and trust boundaries

Shared tool architecture
10 referenced entries · GNU Radio, gr-satellites, Orekit, Wireshark/TShark, Zeek. Native evidence and reporting components complete the cluster.

Quantum readiness

6 stages

Under testing

A cryptographic asset inventory supports algorithm and dependency review, exposing the evidence needed to assess migration readiness.

Assessment scope
Cryptographic discovery and migration readiness analysis

Shared tool architecture
6 referenced entries · Cirq, Qiskit SDK. Native evidence and reporting components complete the cluster.

88 Core + 13 C2 continuation + 80 Advanced + 17 Ultimate = 198 stages.

Under testing

UNDER TESTING

Physical and industrial systems

Hardware / firmware

9 stages

Under testing

Firmware images and component inventories support metadata, provenance and secure-boot review. Image, component and boot-policy evidence remain distinguishable.

Assessment scope
Firmware metadata, component provenance and secure-boot posture

Shared tool architecture
11 referenced entries · Binwalk, Cosign, Ghidra, ipsw, LLVM binary utilities, QEMU, Syft, Trivy. Native evidence and reporting components complete the cluster.

ICS / SCADA

9 stages

Under testing

Industrial asset and configuration records support protocol and segmentation review. Asset, protocol and zone context define the relevant branches.

Assessment scope
Configuration review, protocol records and segmentation posture

Shared tool architecture
11 referenced entries · OpenSCAP, QEMU, Suricata, Wireshark/TShark, Zeek. Native evidence and reporting components complete the cluster.

88 Core + 13 C2 continuation + 80 Advanced + 17 Ultimate = 198 stages.

Under testing

UNDER DEVELOPMENT

PurpleShades and digital forensics

PurpleShades · Defensive patching

8 stages · **Under development**

Asset and finding intake opens parallel exposure, dependency and remediation analysis. A change plan brings the branches together with rollback criteria, canary observations and approval requirements.

Advisories → assessment branches → change proposal → rollback / canary criteria → approval → review packet

The workflow assembles a reviewed proposal and defines the evidence required to validate a future change.

Digital forensics

9 stages · **Under development**

Case intake establishes evidence identity and custody. Artifact, timeline and correlation branches preserve source attribution and converge into a reviewable case record.

Case intake → evidence preservation → analysis branches → correlation → review → case report

Integrity checks precede analysis. Incomplete or conflicting observations remain visible in the final evidence account.

88 Core + 13 C2 continuation + 80 Advanced + 17 Ultimate = 198 stages.

Under development

ANNUAL PRICING PER SEAT

Annual pricing and bundle entitlements

Each annual seat brings the native workspace, integrated tool workflows and controlled model access together. Select the assessment scope and deployment entitlement that fit the work.

Core

Starting at

$7,000

/ year per seat

88 Core stages + 13 C2 continuation stages

Validated Core

100 fine-tuned specialist adapters for bounded stateless calls and code-review roles. Gated 30B3A Flash access includes 50,000 credits per week throughout the active annual subscription.

Advanced

Starting at

$14,000

/ year per seat

Core stage scope + 80 Advanced stages

Under testing

Fine-tuned 30B3A Flash model weights included under NDA for persistent higher-complexity sessions. The weights entitlement gives qualified deployments direct access to the model asset.

Ultimate

Starting at

$20,000

/ year per seat

Core and Advanced stage scope + 17 defensive and forensic stages

Under development

50,000 credits per week throughout the active annual subscription. The proprietary multi-encoder suite adds task-specific embedding and representation variants for defensive and forensic work; it is not an LLM. An optional additional $5,000 weights entitlement under NDA supports intensive parallel and large-network deployments.

Fine-tuned model and adapter access is controlled by subscription gates. Weights access is a separate, selective entitlement under NDA. Active subscriptions receive applicable weights and stage updates at least every six months.

198 stages: 88 Validated Core + 13 C2 continuation + 80 Advanced + 17 Ultimate.

88 Core + 13 C2 continuation + 80 Advanced + 17 Ultimate = 198 stages.

Annual pricing per seat