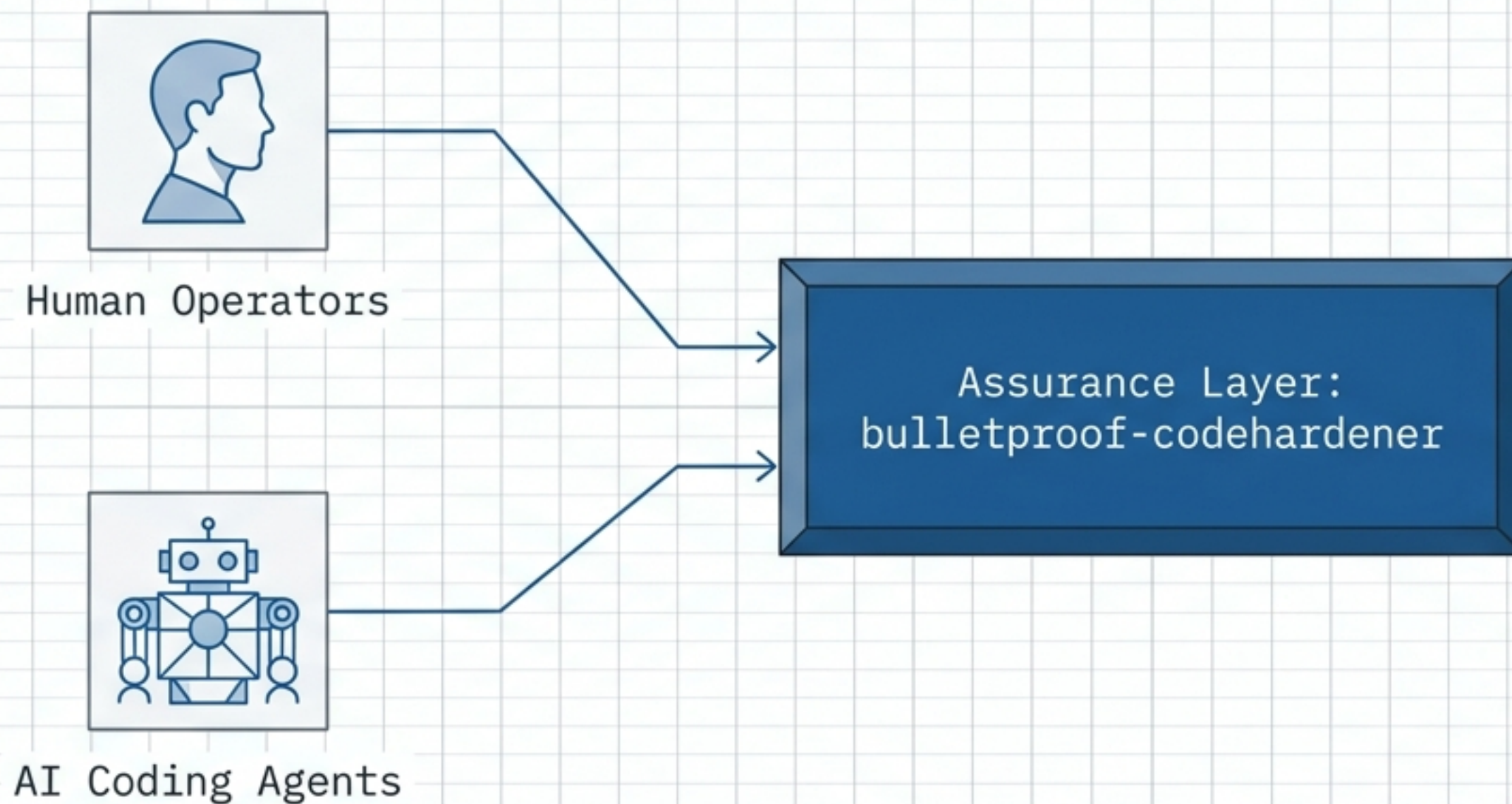
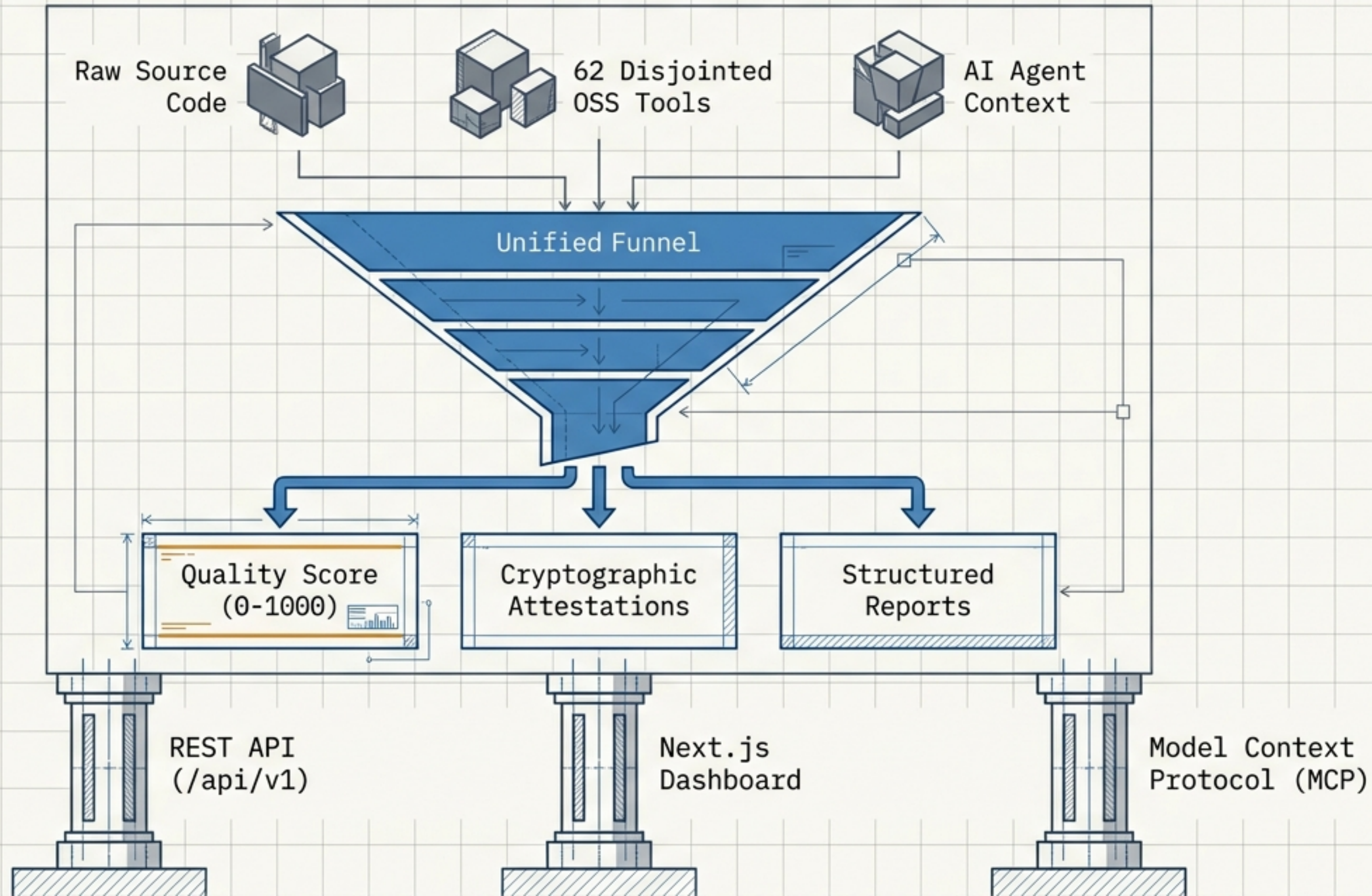


bulletproof-codehardener – System Overview

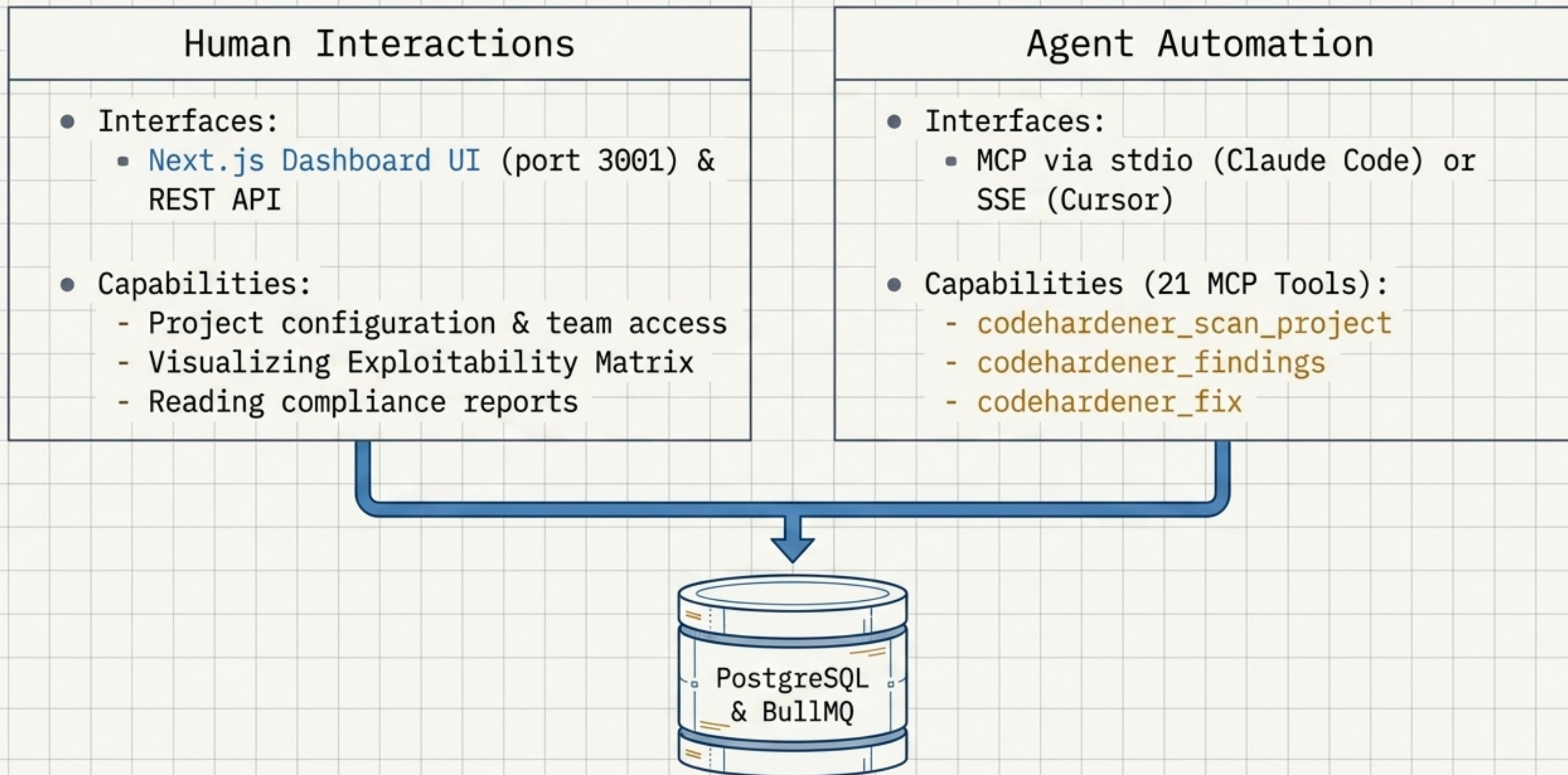


A Unified Security Assurance Platform for AI-First Teams

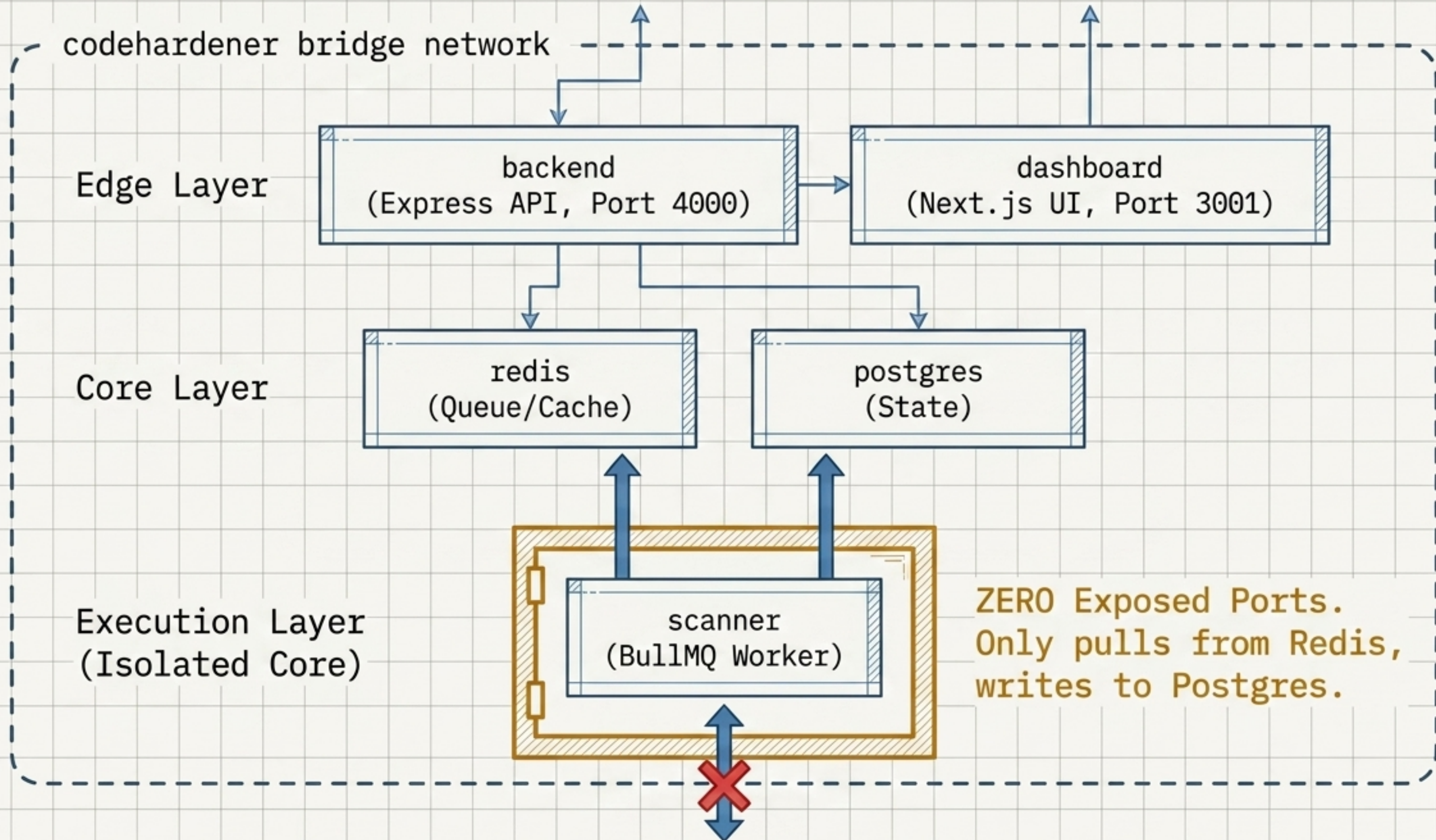
Zero-configuration pipeline wrapping 62 tools, LLM analysis, and cryptographic attestation.



Bridging Human Workflows and Agent Automation

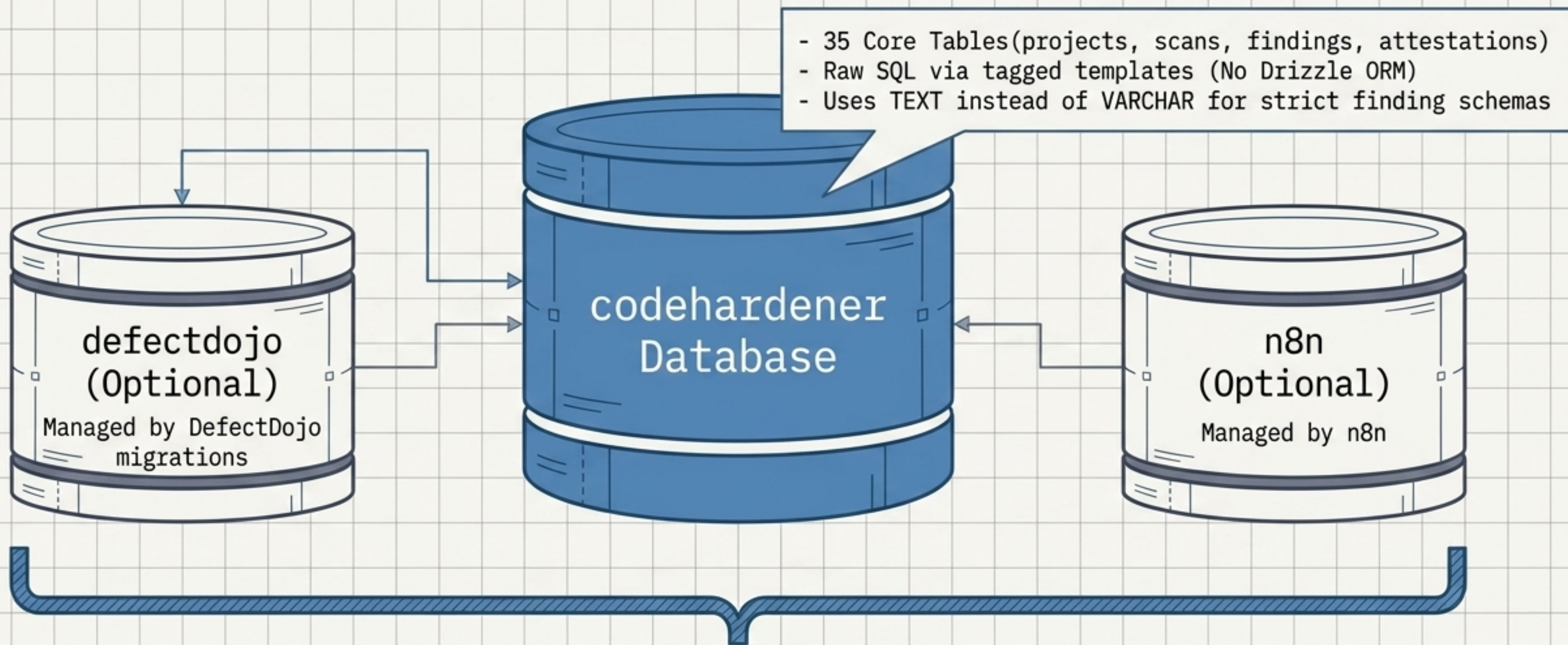


Docker Compose Topology & Network Isolation



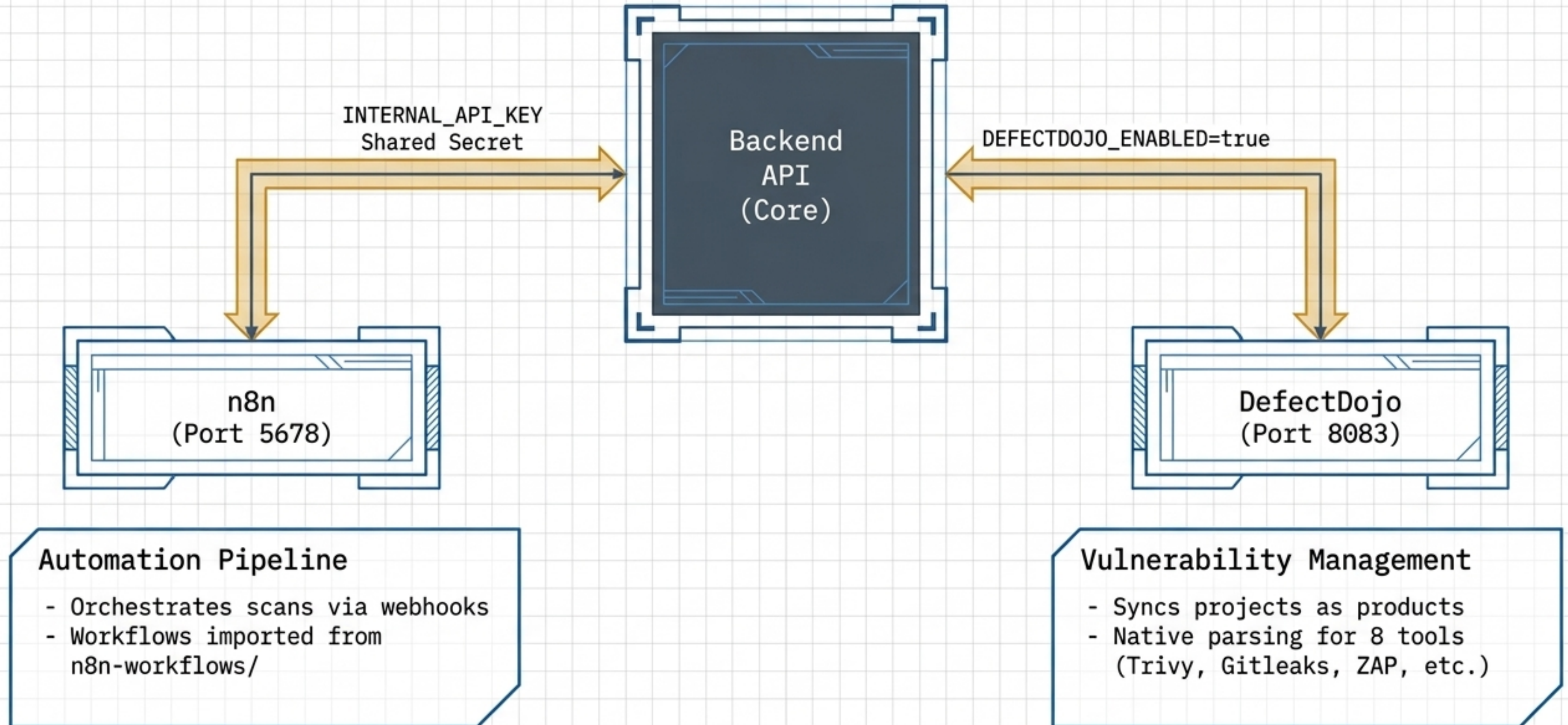
Core State Management in PostgreSQL 16

Self-contained schema tracked via init.sql without ORM overhead.



Single PostgreSQL 16 Host Container (Port 5432)

Enterprise Extension & Workflow Automation



The Scanner Registry: 62 Tools, One Unified Pipeline

SAST (5)

Opengrep
Bandit
Gosec
ESLint Security
PMD

DAST (2)

Nuclei
OWASP ZAP

SCA & Container (3)

Trivy
Grype
Dockle

Secrets (1)

Gitleaks

API & Browser (9)

Newman
Pact
RESTler
Playwright
Pa11y
etc.

Supply Chain & CI/CD (8)

Syft
in-toto
Cosign
Actionlint
Kubeconform

AI Code Quality (3)

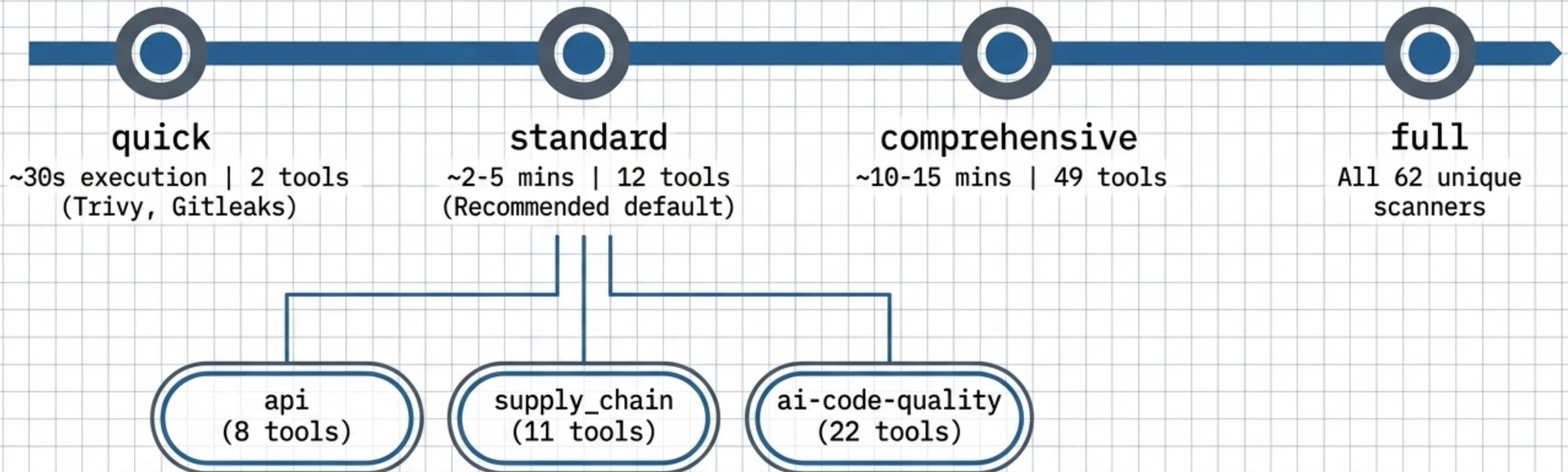
DeepEval
package-validator
STRIDE

All tools synthesize into 37 distinct analyzers (22 quality, 15 security) emitting a single unified finding schema.

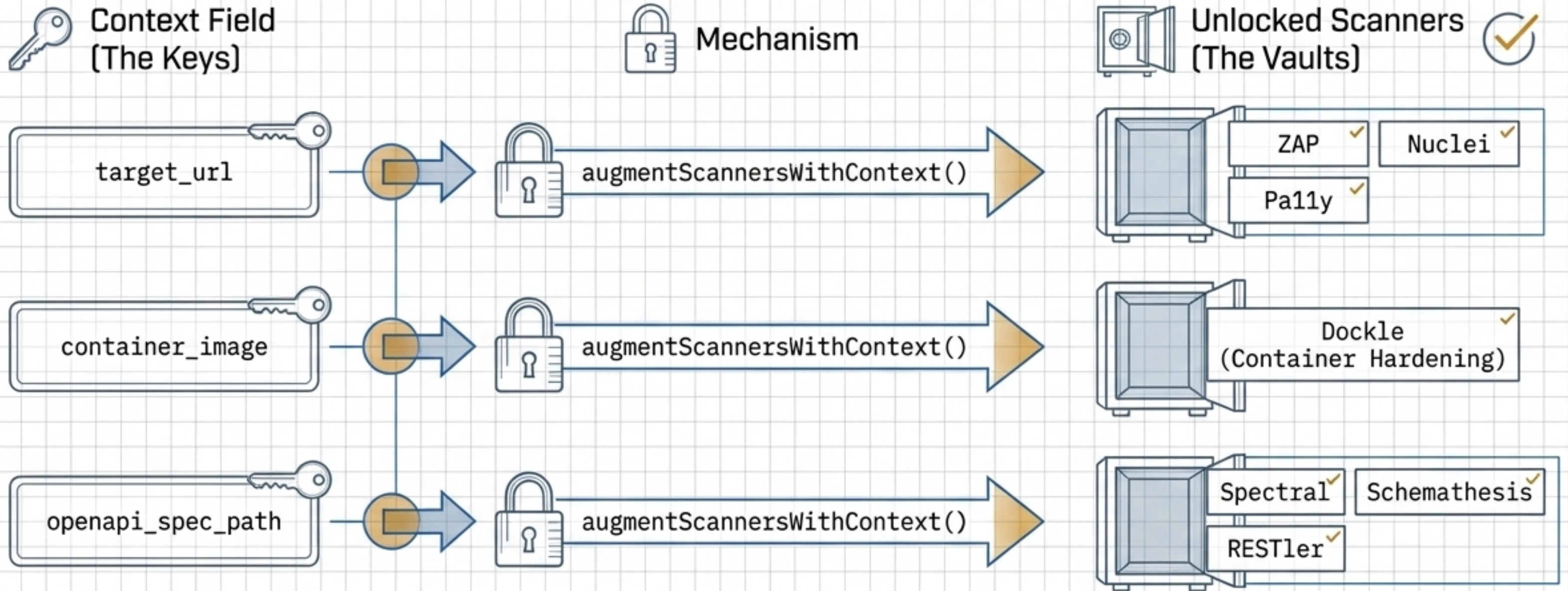
Intelligent Scan Profiles



Auto-Detection Sensor:
'auto' profile dynamically detects
languages (CA-001) and selects
scanners. Falls back to standard.



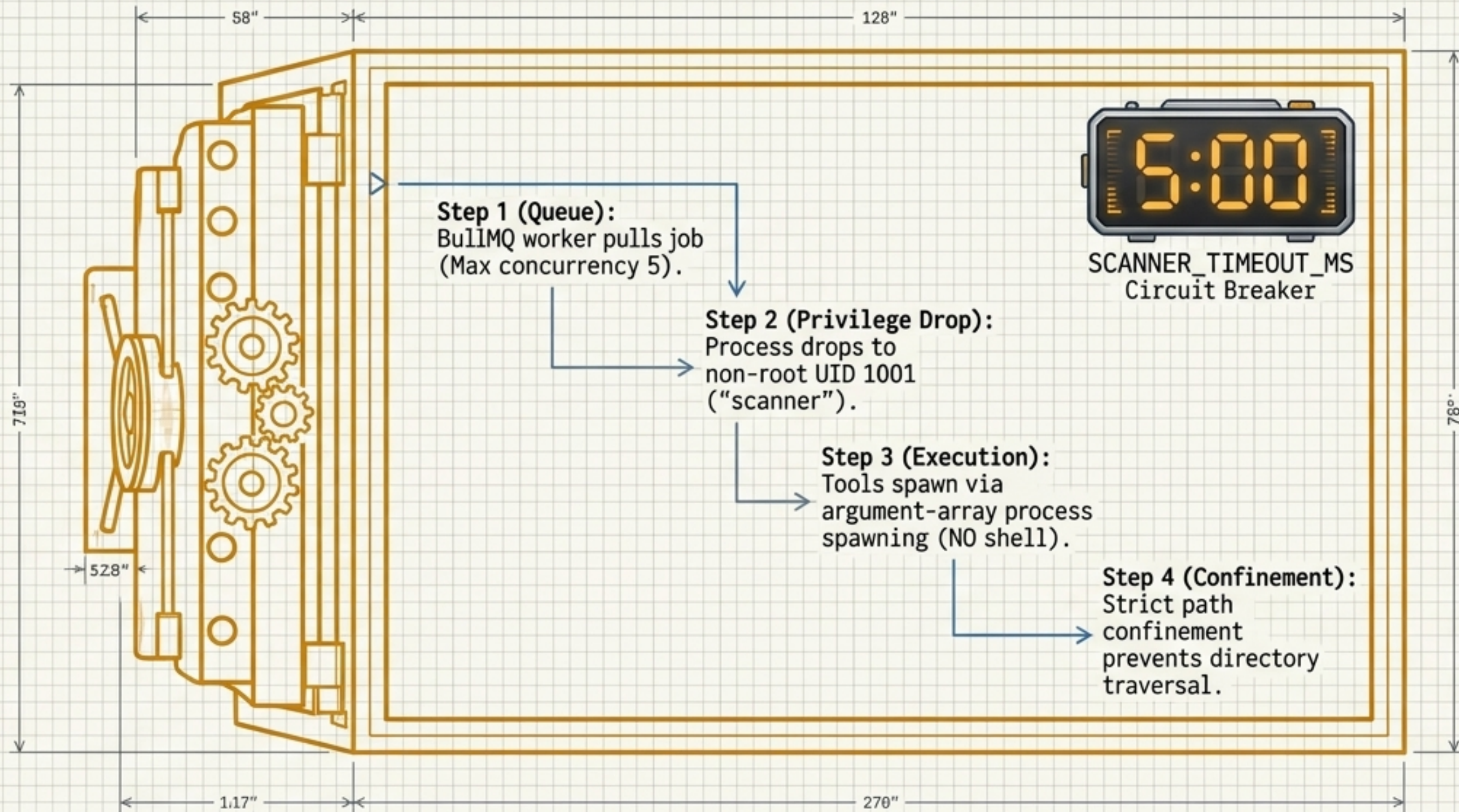
DAST Context & Scanner Maximization



Missing context results in a structured **skipReason** visible in the Dashboard UI.

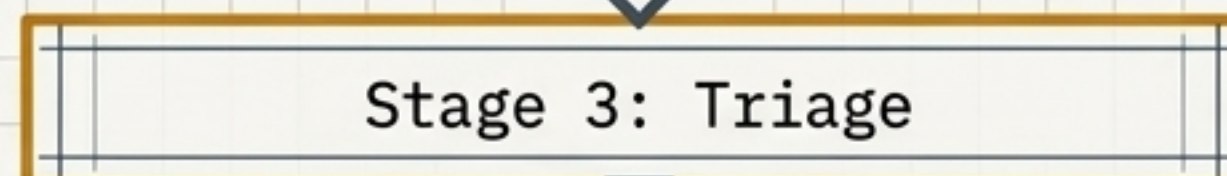
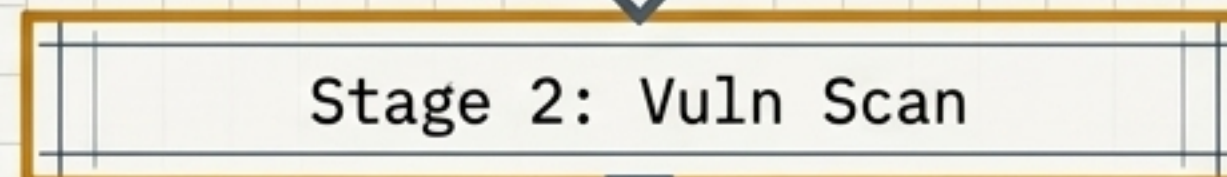
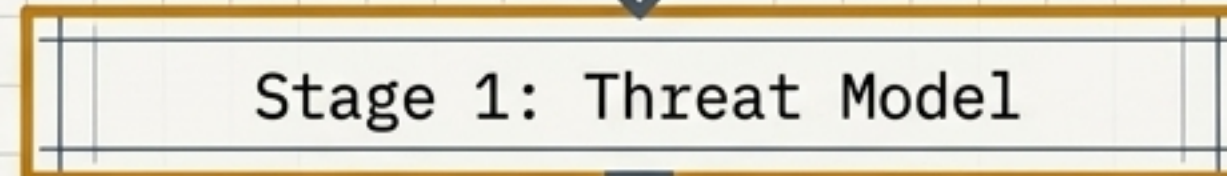
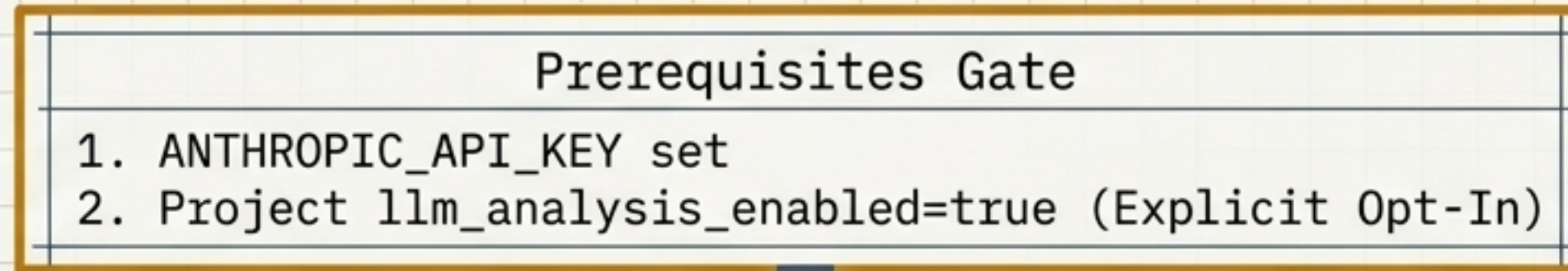
Scanner Container Isolation

Secure execution of untrusted code and tools.

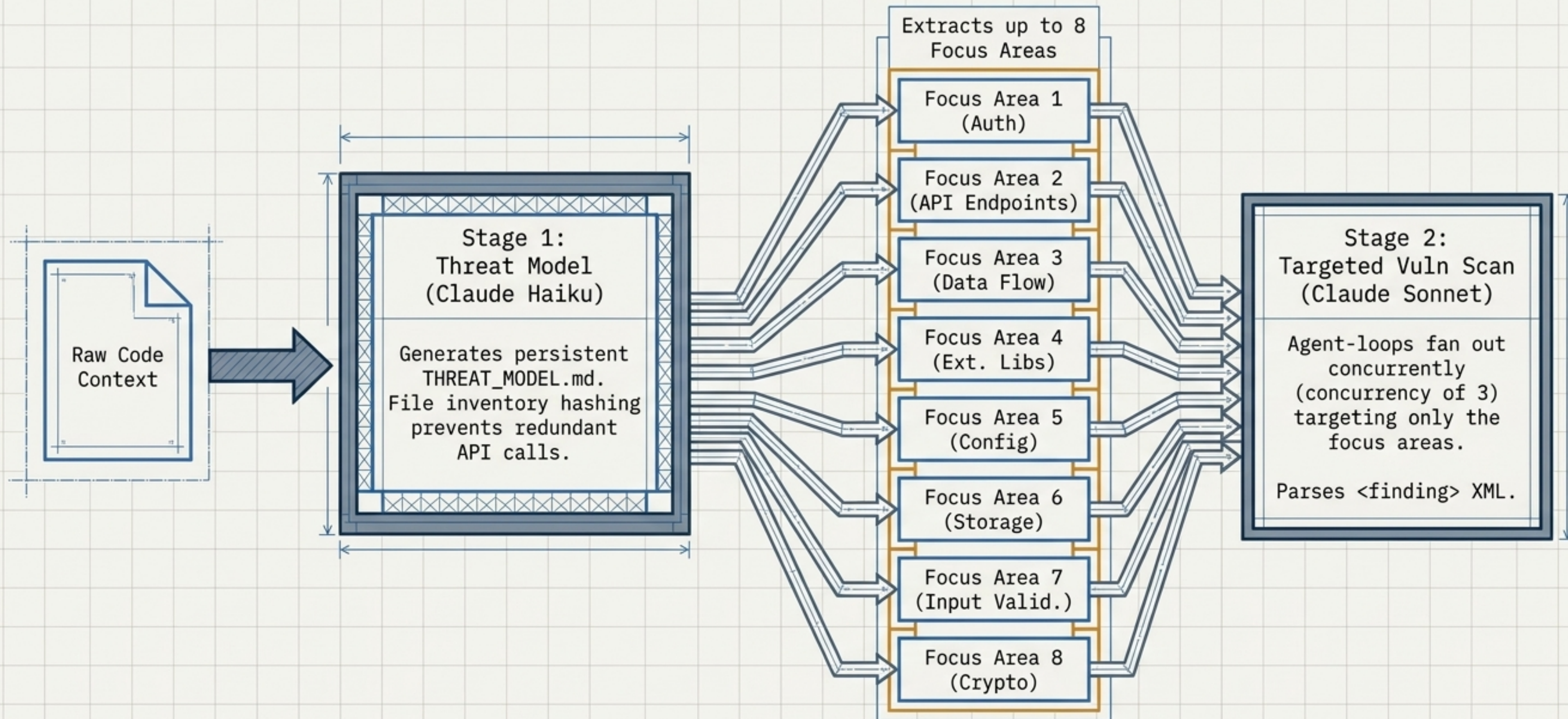


The LLM Assurance Layer

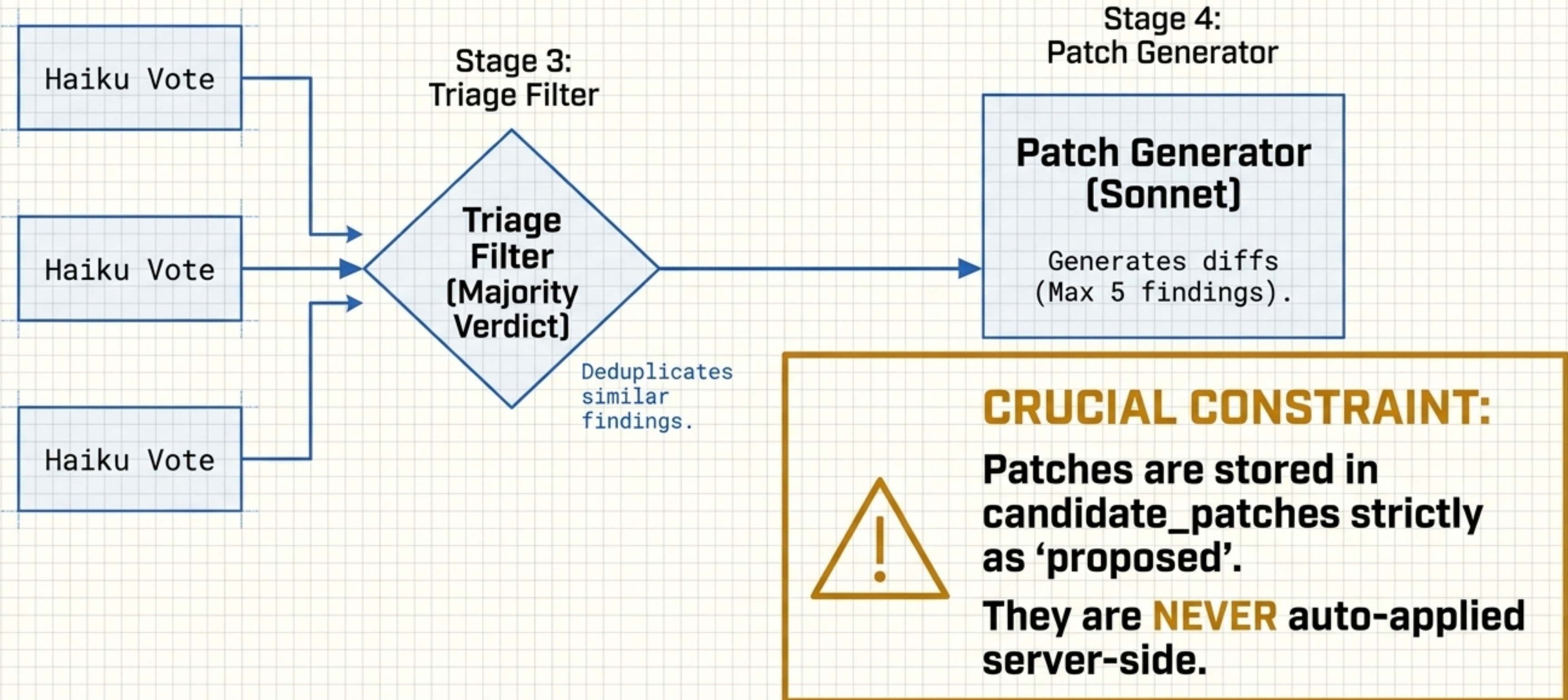
Premium 4-stage static analysis pipeline integrated via defending-code-reference-harness.



Stage 1 & 2: Context-Aware Threat Modeling



Stage 3 & 4: N-Vote Triage & Patch Generation



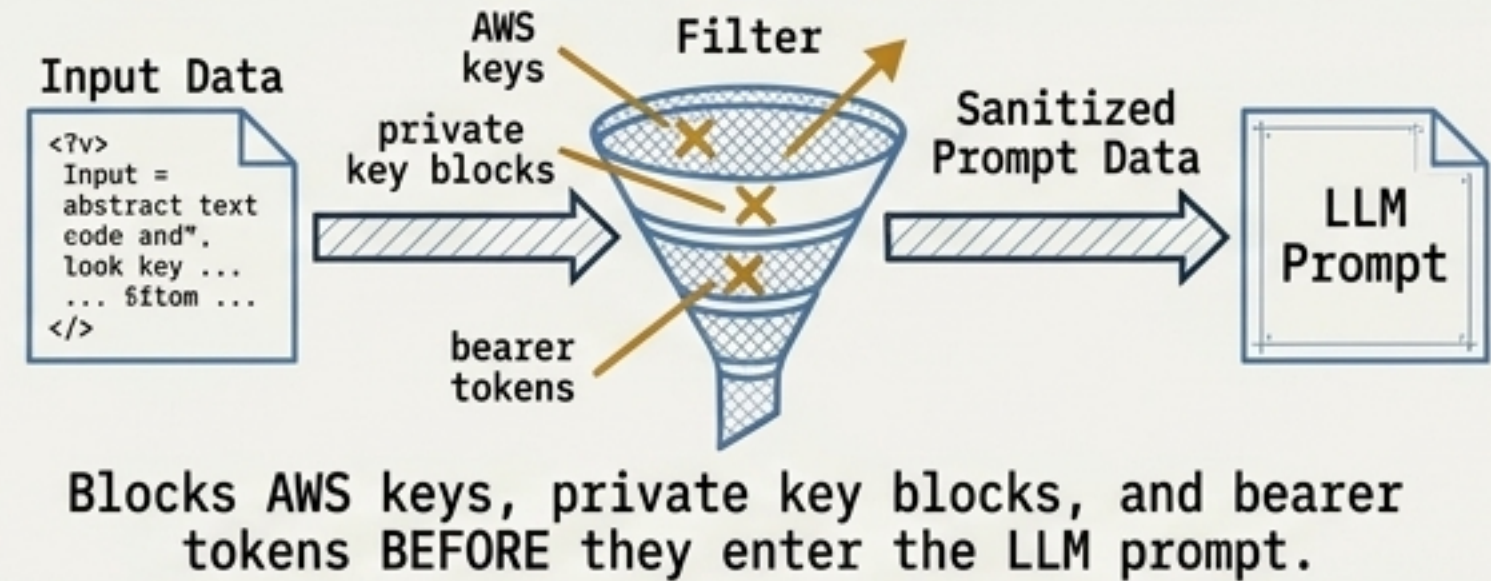
Strict Guardrails: Security & Cost Controls

Safeguards governing Anthropic API integrations.

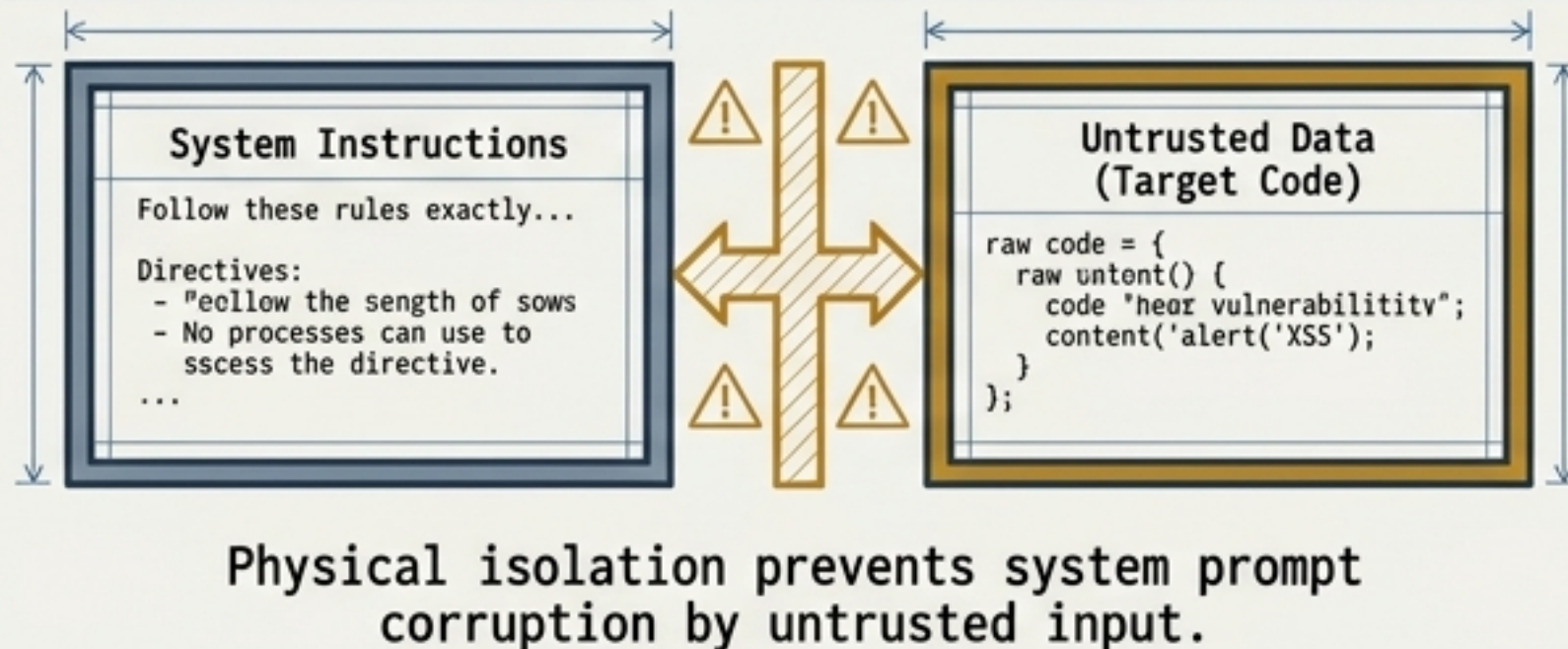
Token Budget



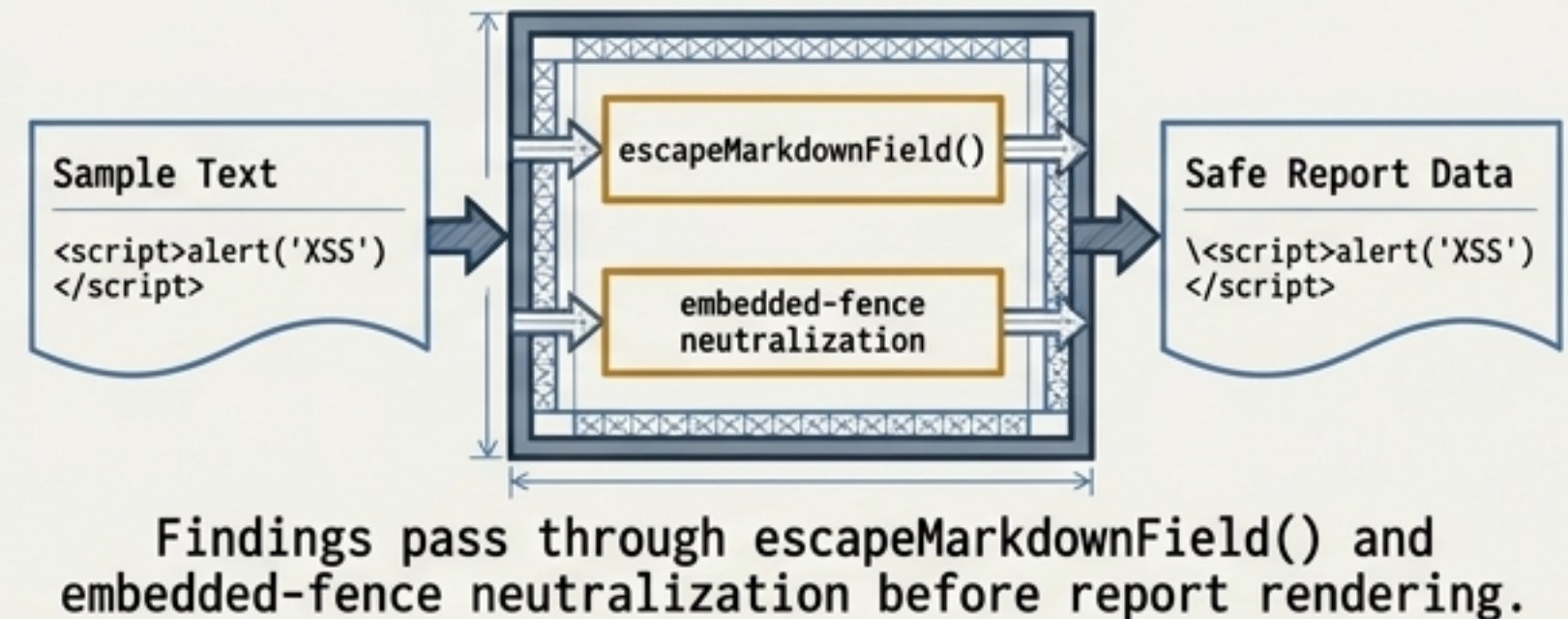
Regex Secret Redaction



Untrusted Framing

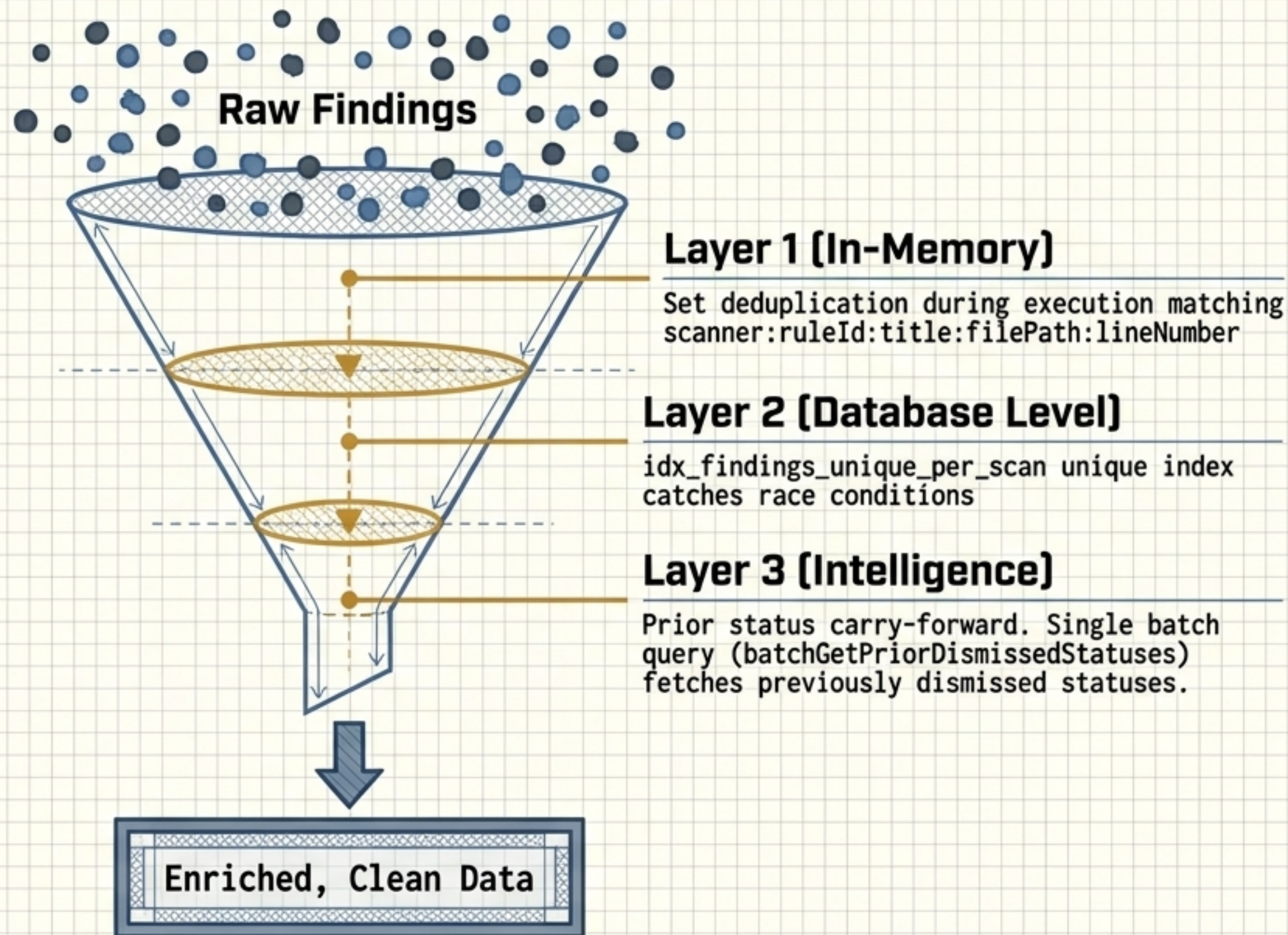


Markdown Injection Safety



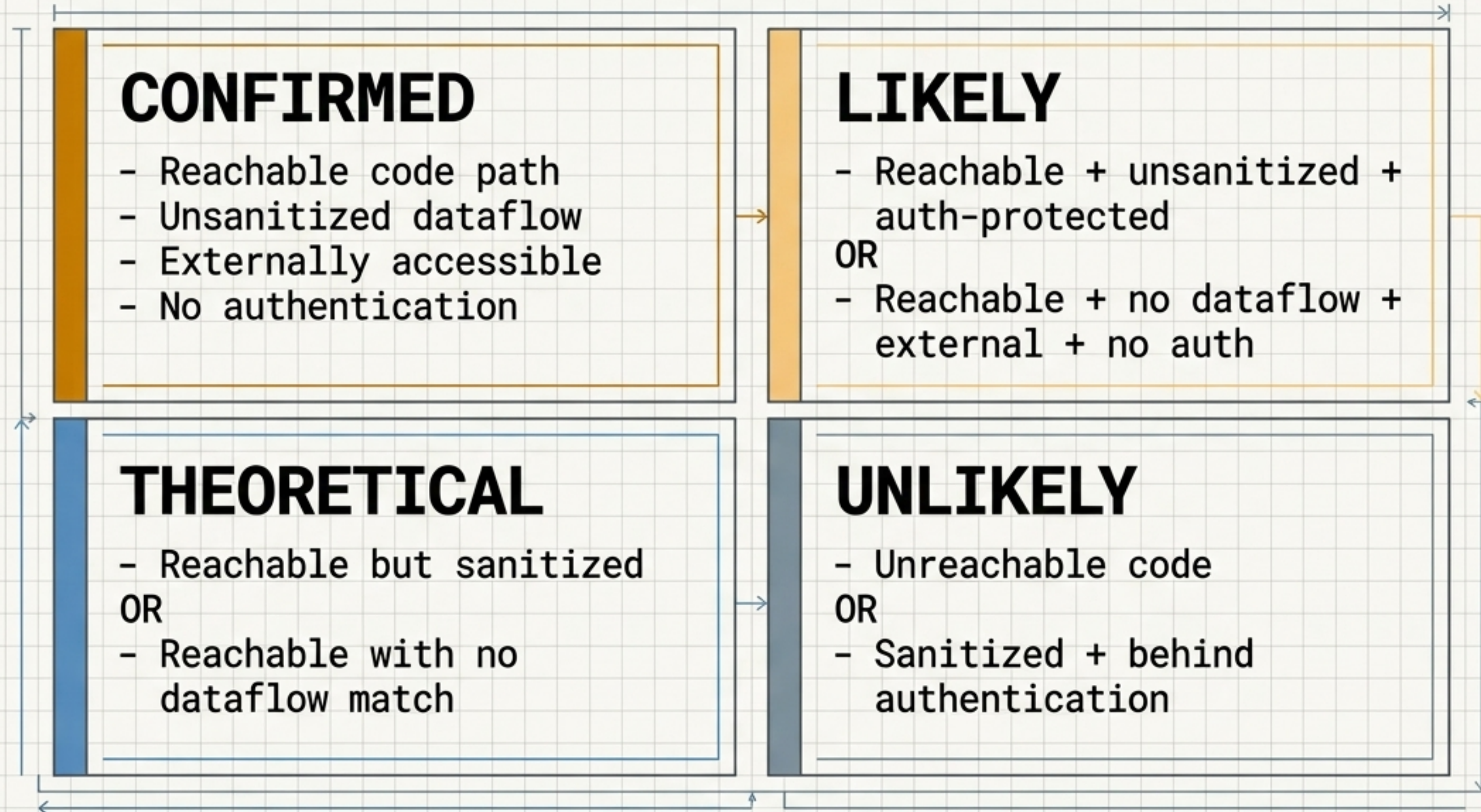
The Finding Enrichment Pipeline

Reducing false positives from 62 standard tools through intelligence.



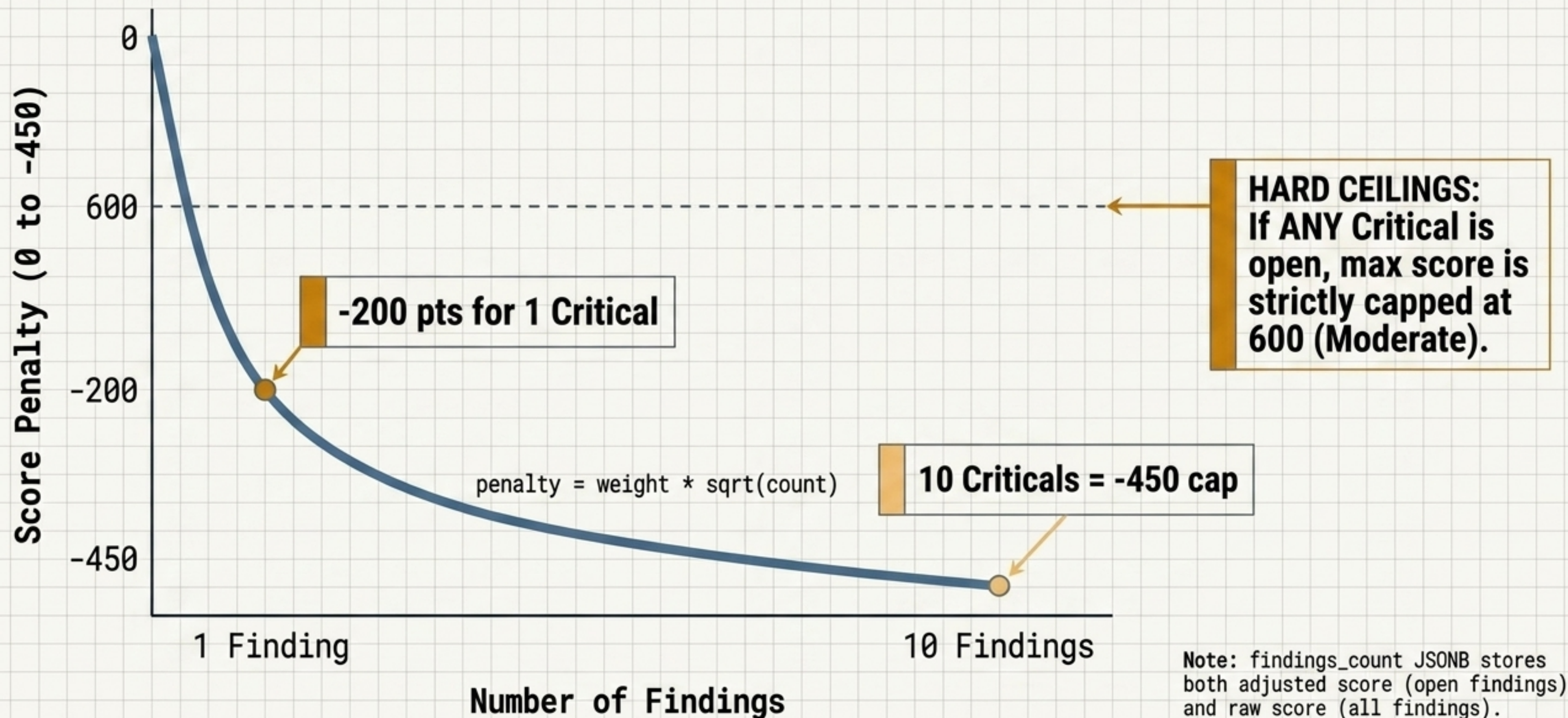
Classifying True Risk: The Exploitability Matrix

A diagnostic grid for assessing exploitability based on data logic.



The Quality Score Engine (0-1000)

A diagnostic grid for assessing exploitability based on data logic.

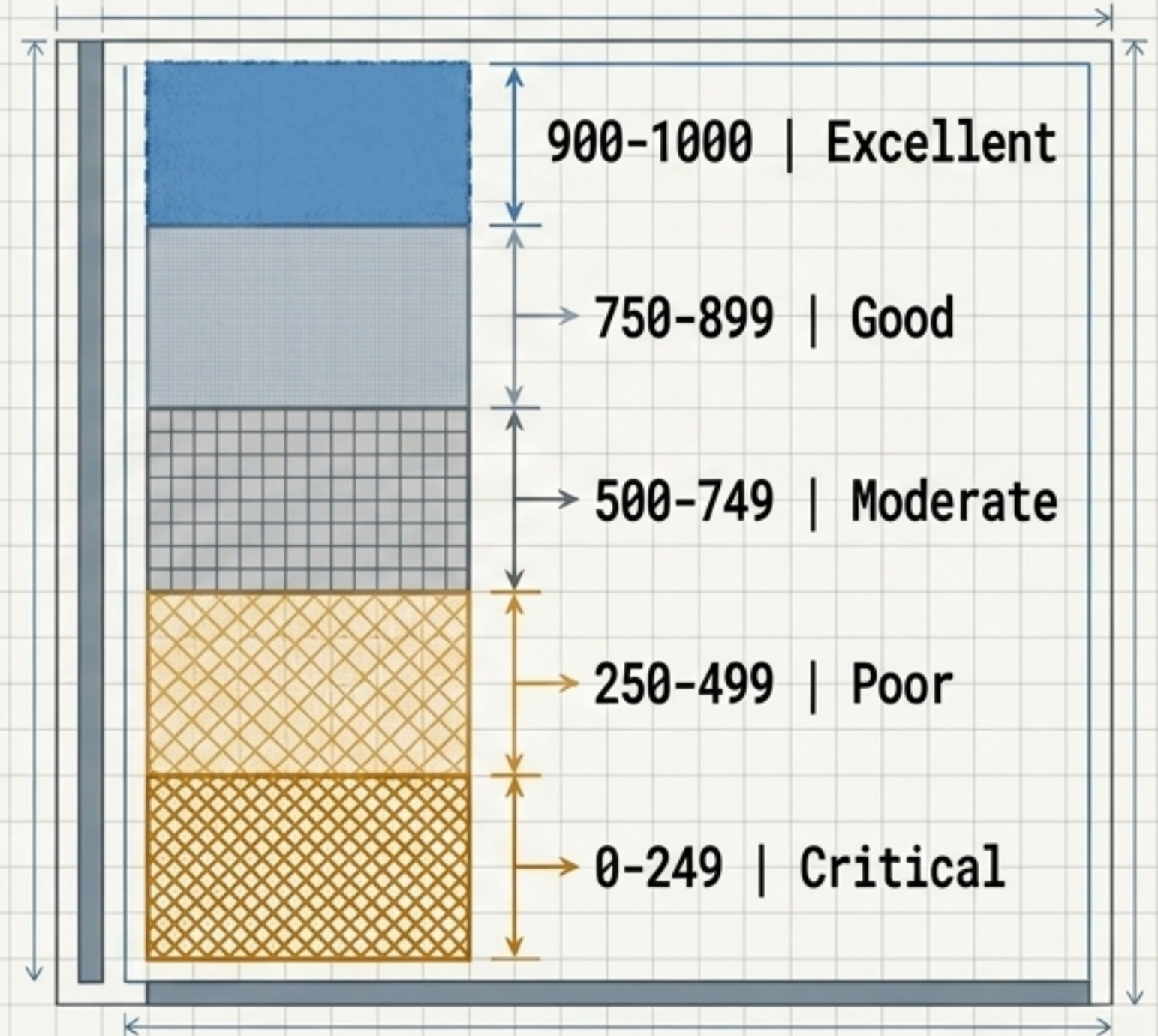


Incentivizing Hygiene: Quality Bonuses & Tiers

Achievement Board (Max 280 pts)

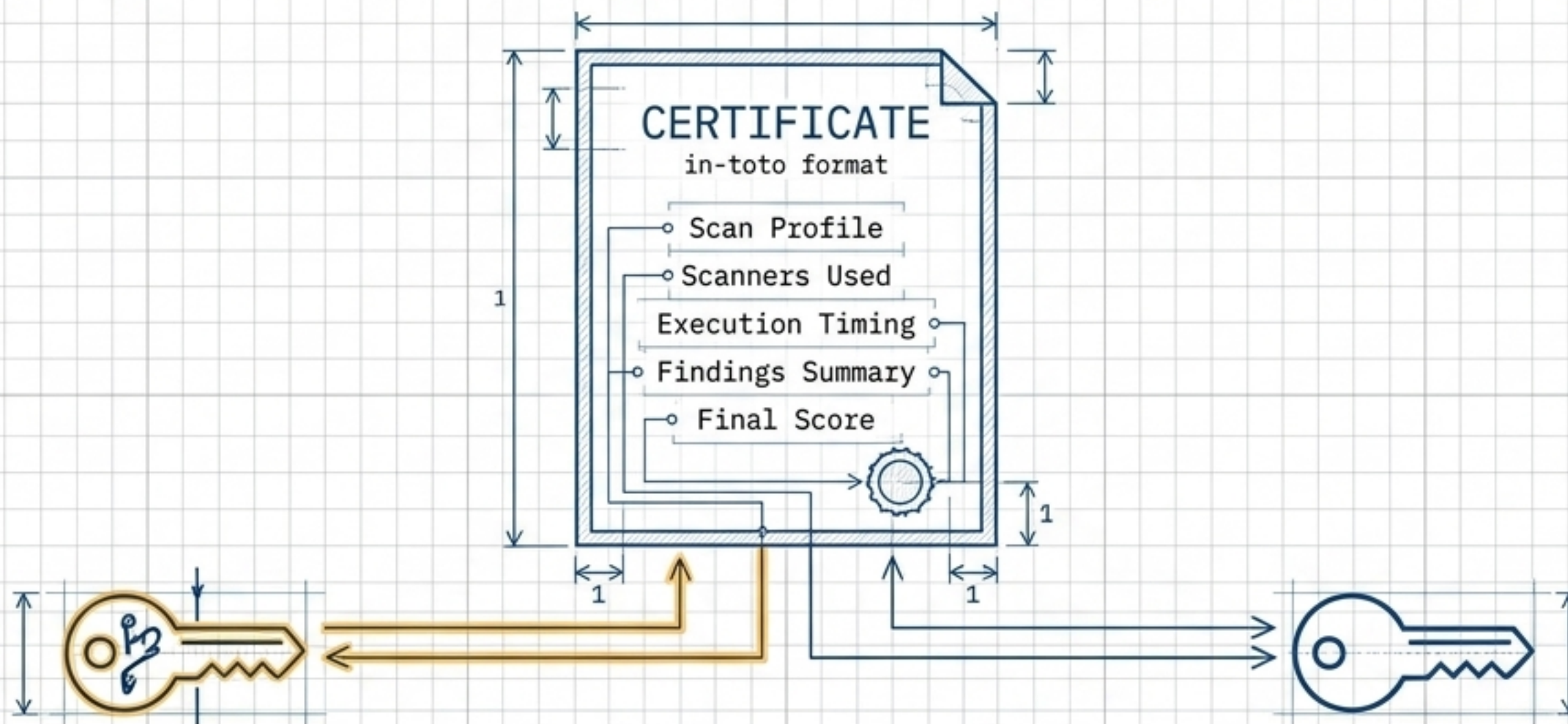
✓	SBOM Generated	+25 pts
✓	Signed Attestation	+30 pts
✓	All Tests Passing	+30 pts
✓	No Confirmed Exploits	+25 pts

Quality Levels Scale



Cryptographic Attestation & Provenance

Supply chain provenance mathematically proving the work of every scan.



1. Sigstore (Preferred)

Cosign keyless signing via Fulcio CA.
Logged directly to the Rekor transparency log.

2. Ed25519 (Fallback)

Local key pair generation
(attestation-signing.pem).

Portable Outputs: Reports & Badges

Embeddable Badges

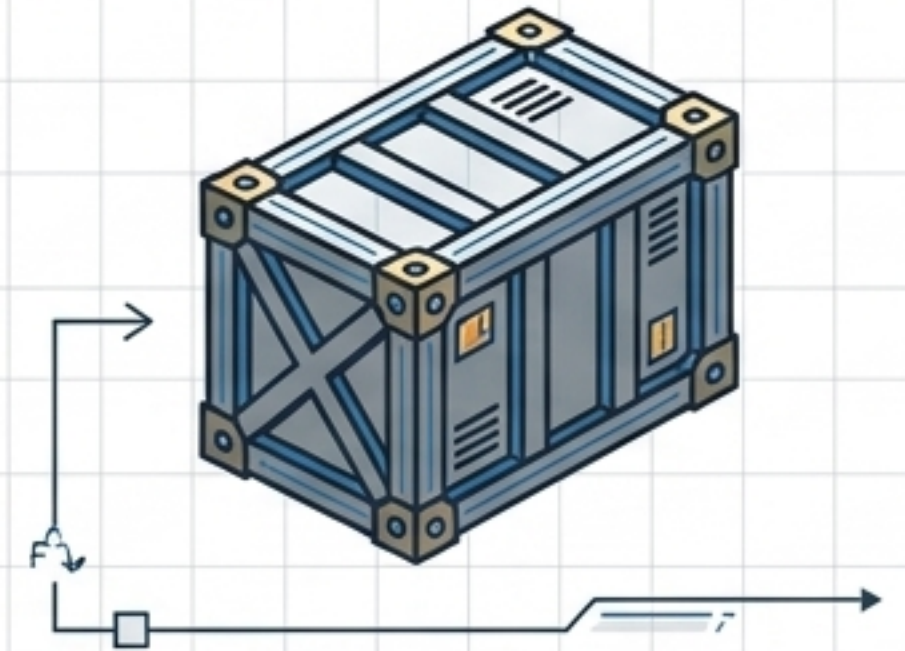


Structured Reports



- Markdown
- SARIF (CI/CD ingestion)
- JSON
- PDF

SBOM Generation



CycloneDX Software Bill of Materials. Maps directly to the **codehardener_sbom** MCP tool.

Administrator Summary

The Platform Mandate

- ✓ **Deploy:** **Docker Compose** (.env configured, minimum 6GB RAM)
- ✓ **Interface:** **REST API**, **Next.js UI**, **MCP** (stdio/SSE)
- ✓ **Execute:** **62 tools** safely isolated in the scanner container (**UID 1001**)
- ✓ **Analyze:** **Optional LLM** deep scanning with strict token/path guardrails
- ✓ **Store:** State safely preserved in **Postgres 16**; transient jobs in **Redis**

