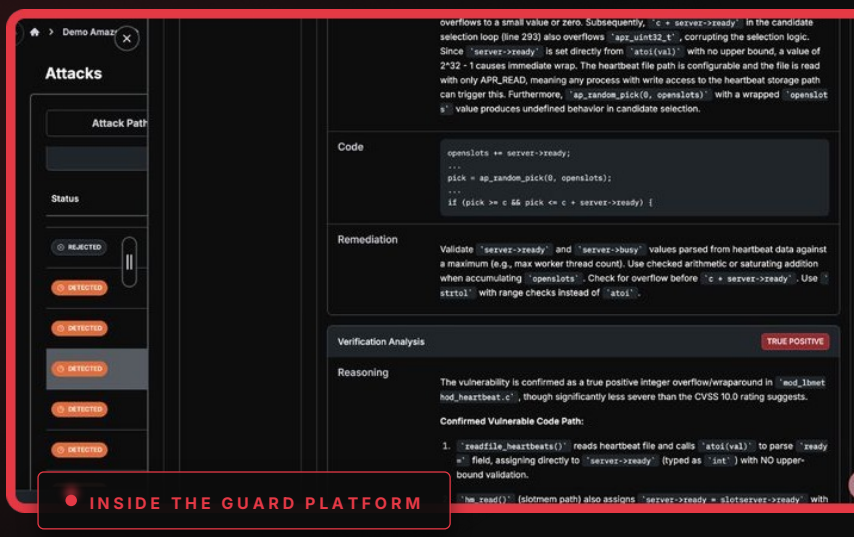
AUTONOMOUS VULNERABILITY DISCOVERY & PATCHING

Constantine

The autonomous auditor that finds, proves, and patches.



AUTONOMOUS CODE AUDITOR // AGENTIC LLM PIPELINE

Find fatal bugs. Prove they're real. Ship the fix.

Point Constantine at a source code repository and get back confirmed, exploitable vulnerabilities. Every finding ships with a patch **already validated against the original exploit**. No human intervention between stages — clone to finding to tested patch runs as a single command inside the Praetorian Guard Platform. Constantine changes the economics of source code security from *hire experts and wait weeks* to *run a pipeline and get results*.

WHY CONSTANTINE IS DIFFERENT

PATCHING > DISCOVERY // 01

Patching matters 3× more than discovery.

Finding a bug is easy. Proving it is real and shipping a correct fix is hard. Every Constantine patch is re-tested against the original exploit before it ships.

NO SPECULATION // 02

Accuracy multipliers punish guessing.

Multiple independent verification stages filter findings so what survives is real. Noise is engineered out of the pipeline — not tuned out after the fact.

THE SIX-STAGE PIPELINE — CLONE → PATCH IN ONE COMMAND

01 · INGEST →

Understand

Clone the repo. Score files 0–100 for security relevance. Focus analysis where it matters.

02 · DETECT →

Scan

LLM scanners flag suspicious patterns, then validate them with deep CWE-specific analysis.

03 · REVIEW →

Verify

Agentic LLM verifier traces data flows. Taint-aware call graphs confirm reachability.

04 · EXPLOIT →

Prove

Sandboxed agent writes, executes, and iterates exploits until the bug is proven real.

05 · PATCH →

Fix

Tiered repair strategy. Every patch re-runs the exploit. Only validated fixes ship.

06 · REPORT

Deliver

Structured output with full evidence chain. CVSS and CWE included on every finding.

INSIDE THE GUARD PLATFORM · BENCHMARKS · OPERATING MODES

A native capability of Praetorian Guard.

Constantine runs inside the platform you're already paying for — not a separate tool, not a separate contract, not a separate dashboard.

One platform. One workflow. One source of truth. Constantine findings flow directly into the Guard dashboard as Risks, alongside the output of every other Guard capability — Attack Surface Management, Continuous Penetration Testing, Vulnerability Management, Breach and Attack Simulation, and Cyber Threat Intelligence.

Every Risk carries the full evidence chain: detection reasoning, reviewer verdict, exploit proof, and validated patch. You triage, assign, and remediate with the same workflow you already use — the discovery engine underneath just got an order of magnitude better.

GUARD PLATFORM — CAPABILITY STACK

- Attack Surface Management
- Continuous Penetration Testing
- Vulnerability Management
- Breach and Attack Simulation
- Cyber Threat Intelligence
- **Constantine — Code Auditor**

Proven against real-world CVEs.

28 CONSEQUENTIAL VULNERABILITIES · 6 LANGUAGES

Constantine is benchmarked against **28 of the most consequential vulnerabilities** in modern software — spanning memory safety, authentication bypass, cryptographic flaws, container escapes, and denial of service across C, Java, Python, Go, Rust, and JavaScript. A representative sample:

CVE-2021-44228	**Log4Shell** · RCE via JNDI lookup in Apache Log4j
CVE-2022-0847	**Dirty Pipe** · Linux kernel privilege escalation
CVE-2024-6387	**regreSSHion** · Signal handler race in OpenSSH
CVE-2023-4911	**Looney Tunables** · Buffer overflow in glibc
CVE-2014-0160	**Heartbleed** · Missing bounds check in OpenSSL TLS
CVE-2021-3156	**Baron Samedit** · Heap overflow in sudo
CVE-2022-21449	**Psychic Signatures** · ECDSA verification bypass in Java
CVE-2024-21626	**runc Container Escape** · FD leak to host filesystem

TWO WAYS TO PUT IT TO WORK

MODE 01 · PRIVATE

Customer Private Repositories

Connect Constantine to a private repo. Findings land in the Guard dashboard as **Risks**, integrated with your existing triage and remediation workflows. Every Risk carries the full evidence chain.

`detection` `reviewer verdict` `exploit proof` `validated patch`

MODE 02 · PUBLIC

Make Me Famous

Point Constantine at any public repository — OpenSSL, nginx, Node.js, curl. A Praetorian analyst reviews the results and coordinates **responsible disclosure**. Offense informing defense, at scale.

`OpenSSL` `nginx` `Node.js` `curl` `+ your pick`

COVERAGE

ANY REPO, ANY REF

Constantine works on **any git repository** — public or private, GitHub or GitLab, monorepo or single service. Scan an entire repo at a ref, a specific pull request, or a commit range. The LLM scanners are language-agnostic and have been validated against major production languages.

`C` `C++` `Java` `Python` `Go` `Rust` `JavaScript`

See Constantine inside Guard.

Book a scoping call — we'll scan a repo of your choosing on the call.

REQUEST A GUARD DEMO →