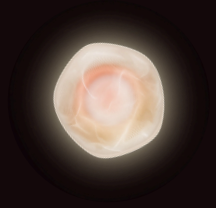
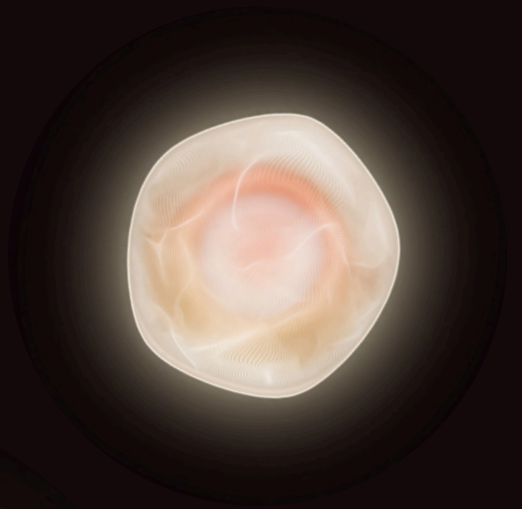
Your exposure programme is only as strong as its weakest dimension.

Most CISOs know their programme is not where it needs to be. The harder question is knowing exactly which part of it is holding everything else back and what fixing that one thing would unlock across remediation speed, validation confidence, and leadership visibility.

The gap is rarely about resources. Organizations at every maturity level carry the same frustration: tools deployed and processes defined, yet the remediation backlog grows, findings pile up faster than anyone can validate them, and the board wants answers the programme cannot yet give.

The reason is structural. External exposure management has four distinct operating postures. Most organizations are stronger in some dimensions than others. The weakest dimension sets the ceiling for everything above it. Until that gap is identified and closed, advancement stalls regardless of what else changes.





What the model is

The Hadrian Exposure Maturity Model maps four stages of external exposure management, from reactive and undiscovered to continuous and autonomous. Each stage is a recognizable operating posture built from real programme patterns, not an aspirational framework. The model uses seven operational dimensions to tell you where you actually are and what operational bottleneck is holding you back.

WHY MATURITY PROGRESSION MATTERS

STAGE 1 TO 2

MTTR drops from 90+ days toward 45. Coverage rises from below 20% to 40-60%.

STAGE 2 TO 3

True-positive rates rise to 40-60%. SLA compliance reaches 60-80%. MTTR compresses to 15-45 days.

STAGE 3 TO 4

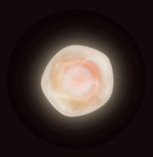
Coverage exceeds 95%. Critical exposures close within 48 hours. Exploit disclosures confirmed in hours, not days.

THE THREAT LANDSCAPE IS NOT WAITING

The average time between vulnerability disclosure and active exploitation has dropped from 32 days to 5. Nearly one in three vulnerabilities is now exploited on or before the day it is disclosed.

Most security programmes are built around weekly triage cycles and quarterly testing. The gap between attacker velocity and programme maturity is not a future risk. It is happening now.

The four stages



STAGE 1

Running Blind

Exposure is discovered reactively. Ownership is unclear. The remediation queue grows faster than it shrinks. The team spends most of its capacity on findings that turn out to be irrelevant.

- Reactive discovery
- No systematic asset ownership
- CVSS-driven triage
- Compliance-focused reporting

STAGE 2

Better Scope, More Hope

The programme is structured and coverage is improving. The constraint is validation: exploitability is assumed from severity scores rather than confirmed. MTTR sits at 45-90 days.

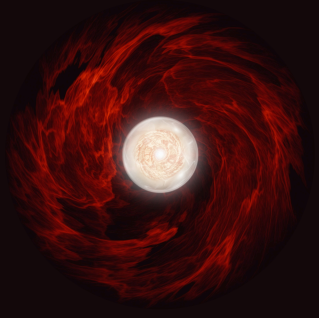
- Scheduled pentests
- Known asset coverage
- Manual exploitability investigation
- Activity-based metrics

STAGE 3

Connecting the Dots

Findings are validated before they reach the queue. True-positive rates reach 40-60%. MTTR compresses to 15-45 days. The constraint is connecting findings into a full attack picture without significant manual orchestration.

- Continuous monitoring
- Automated validation
- Integrated remediation routing
- Exploitable risk measurement

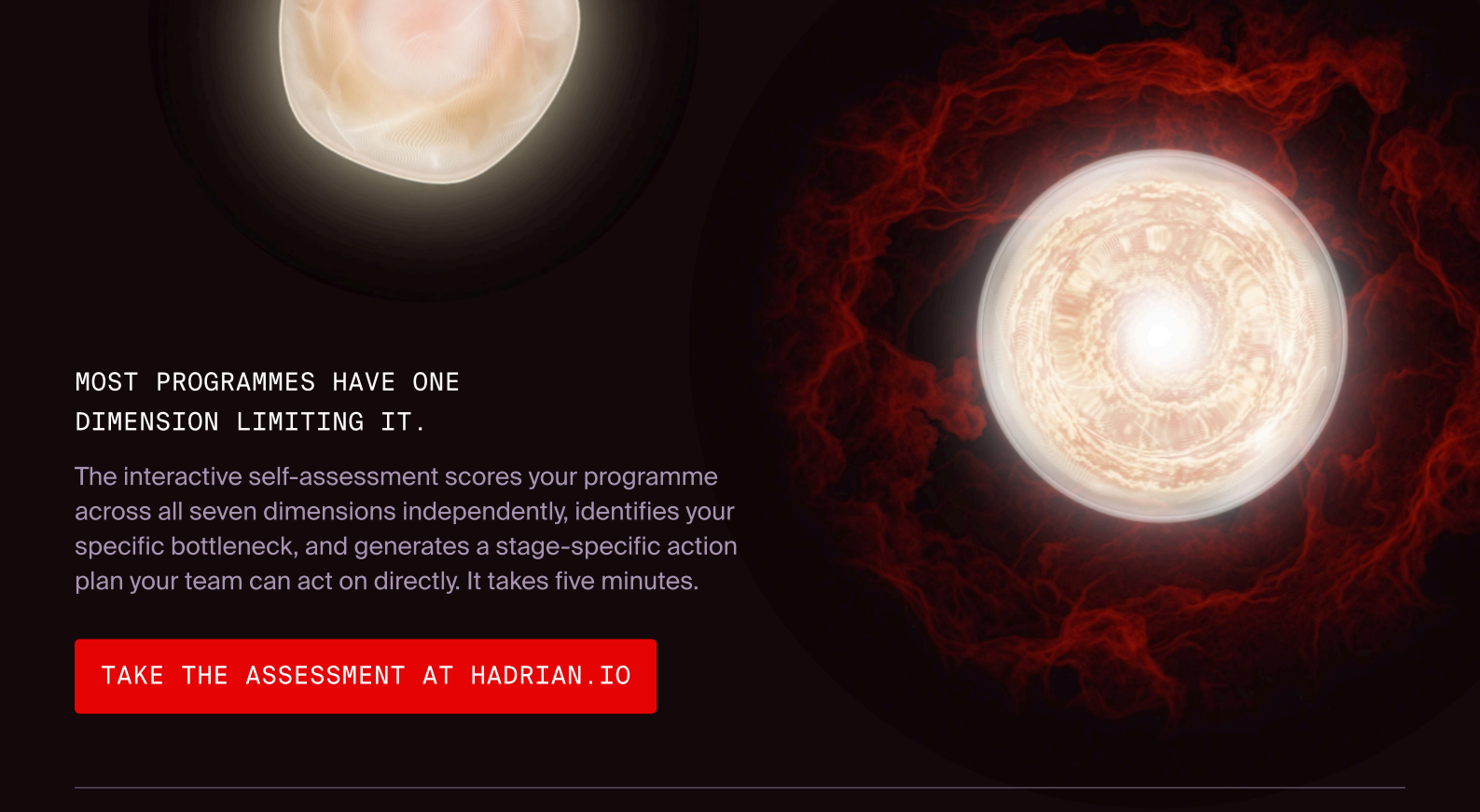


STAGE 4

Clear Picture

Discovery is continuous, validation is autonomous, leadership sees live posture data. Coverage exceeds 95%. Critical exposures close within 48 hours. New exploits confirmed within hours.

- Autonomous emulation
- Real-time posture visibility
- Predictive prioritisation
- Live board reporting



MOST PROGRAMMES HAVE ONE DIMENSION LIMITING IT.

The interactive self-assessment scores your programme across all seven dimensions independently, identifies your specific bottleneck, and generates a stage-specific action plan your team can act on directly. It takes five minutes.

TAKE THE ASSESSMENT AT HADRIAN.IO

ABOUT HADRIAN

Hadrian is an offensive security platform that finds and validates external exposure the way an attacker does — starting from no predefined scope, following attack paths wherever they lead, and confirming every finding as real before it reaches your team. Recognised in the Gartner Hype Cycle for Security Operations, and by GigaOm and Frost & Sullivan.

LEARN MORE: HADRIAN.IO

FROST & SULLIVAN BEST PRACTICES AWARDS

GIGAOM RADAR REPORT LEADER 2025

Gartner Peer Insights 4.9/5 ★

AICPA SOC · ISO 27001

TRUSTED BY 300+ ENTERPRISE ORGANIZATIONS

NBC · amadeus · McKESSON · BLINQX · Crédit Agricole · Leroy Merlin · SHV

ABN·AMRO · London Business School · RITUALS... · SIEMENS energy · LOTTOMatica · FP Francisco Partners · CHRISTIE'S

BIOLANDES · WeatherTech · BLINQX · DAMEN · jamf · exact

ICT GROUP · nedap · celio* · Inova · XM Cyber · AROMA360