HADRIAN

The automation gap

EXTRACT OF HADRIAN'S OFFENSIVE SECURITY BENCHMARK REPORT

INTRODUCTION

Security teams believe they are patching vulnerabilities faster than ever. In reality, they are not. While reported response times suggest rapid remediation, real-world telemetry shows that exploited vulnerabilities often remain unpatched for weeks. This gap between perception and reality creates a false sense of control.

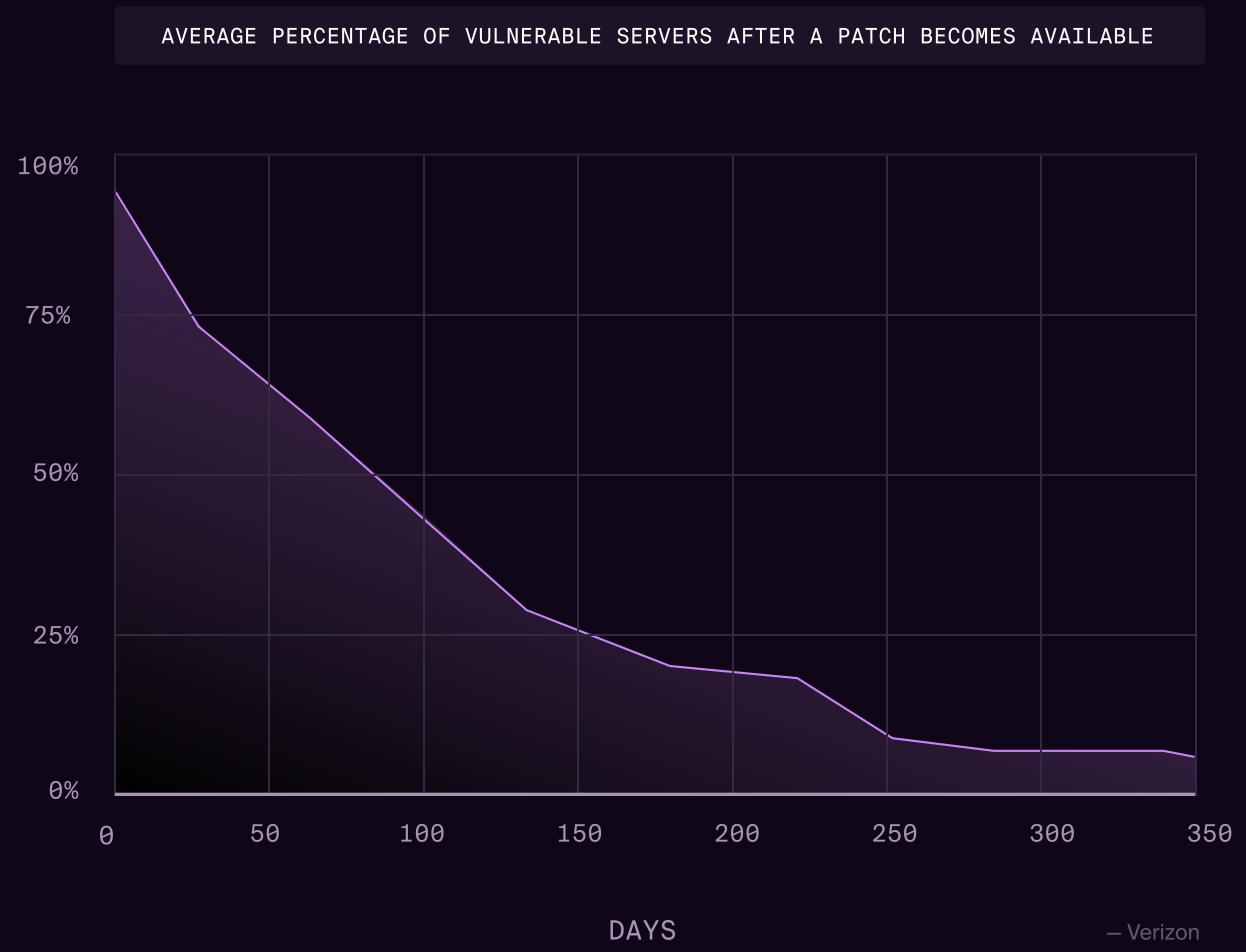
At the same time, AI is accelerating exploitation. Attackers can now discover and abuse exposures faster than security teams can verify and remediate them, especially across short-lived and previously unknown assets. Despite widespread investment in security tooling, validation and response remain largely manual and slow.

The result is an automation gap. Attackers operate at machine speed, while defenders are constrained by visibility-first tools and human workflows. This extract examines how that gap is leaving security teams on the back foot.

The lies we tell ourselves

Zero day response timelines highlight a gap between perceived and actual performance. Ninety four percent of security teams report remediating zero day vulnerabilities within five days, with 47% claiming resolution in one to two days and 7% reporting same day remediation.

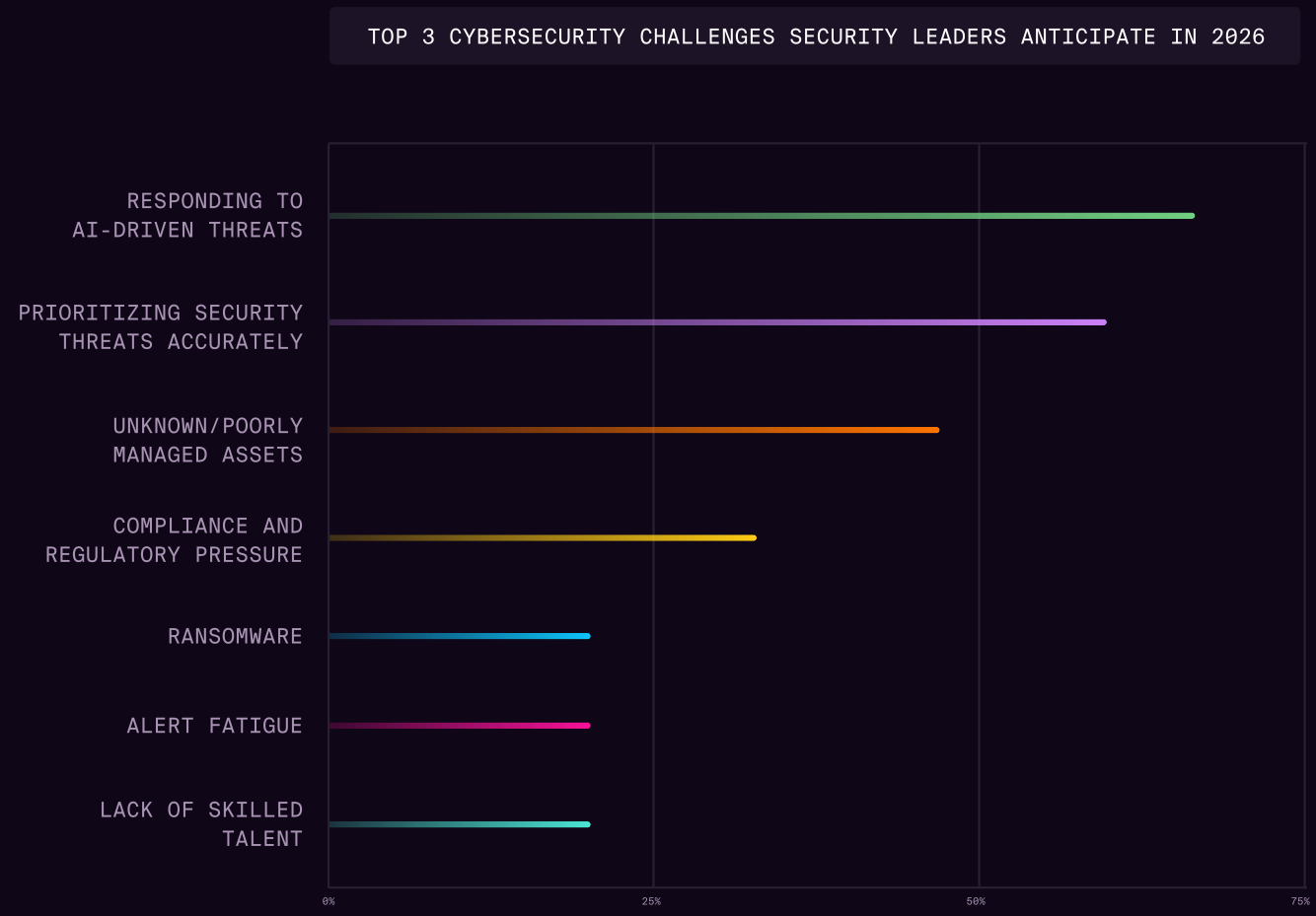
Telemetry tells a different story. According to Verizon, vulnerabilities listed in the Known Exploited Vulnerabilities catalog have a median time to full remediation of approximately 38 days after disclosure. This contrast suggests that confidence in response speed often outpaces what occurs in practice, particularly outside tightly defined zero day scenarios.



AI will drive more exploitation

Responding to AI-driven threats has become the top concern for enterprise security leaders, cited by approximately 67% of respondents. At Hadrian, advances such as Subwiz demonstrate how automation can continuously surface previously unknown and short-lived internet-facing assets that attackers increasingly target.

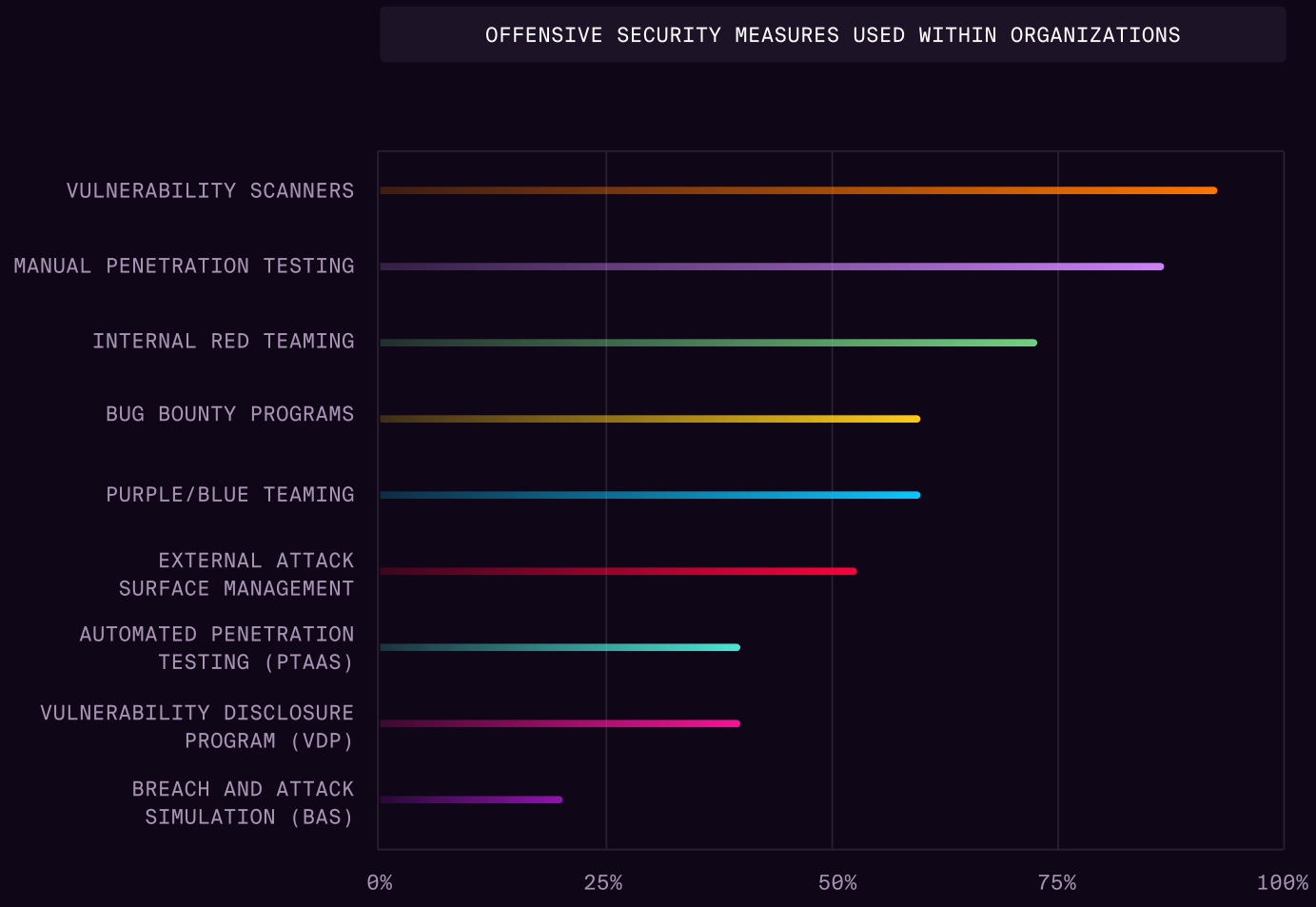
This shift is reflected in recent research from Anthropic. Claude Sonnet 4.5 more than doubled its success rate on Cybench CTF challenges compared with earlier versions and completed complex, multi-step tasks such as traffic analysis and malware decompilation significantly faster than a skilled human. As these capabilities mature and proliferate, AI is expected to play an increasing role in accelerating and scaling data breaches.



Why SecOps can’t break the cycle

Most organizations have invested heavily in security tooling, yet outcomes have not improved proportionally. Ninety three percent of organizations use vulnerability scanners, 87% conduct manual penetration testing, and 73% operate internal red teams. Despite this, only 40% have adopted automated penetration testing. High tool adoption has not translated into faster remediation or clearer prioritization.

This imbalance contributes directly to alert overload. Scanners generate large volumes of findings, while validation remains manual and slow. Teams spend more time managing outputs than reducing risk. The data shows that tooling expansion without automation and verification increases operational friction rather than resilience.



RECOMMENDATION

The data shows that confidence in patching performance routinely exceeds reality, while AI-driven exploitation continues to compress the window for effective response. Relying on manual validation and visibility-first tooling in this environment increases exposure rather than reducing it.

Teams should shift toward automation-first security focused on continuous validation. This means moving beyond detecting vulnerabilities toward automatically validating exploitability, mapping real attack paths, and prioritizing remediation based on live adversary behavior. Exposure management must operate at the same tempo as modern attacks, not at the pace of human review cycles.

This extract highlights only one dimension of the problem. The full Offensive Security Benchmark Report details how automation-driven verification closes the gap between tooling, reality, and outcomes—and what security programs must change to regain the advantage.

Get the full report

ABOUT HADRIAN

Hadrian is an offensive security platform built for teams that need proof, not predictions. We reveal exactly how an adversary could break in today by executing real attacker techniques against your external attack surface. By validating exploitability in production-safe ways, Hadrian eliminates false urgency, sharpens prioritization, and gives teams confidence to act.

Deployed in minutes and engineered for scale, Hadrian seamlessly fits into existing security workflows. Security leaders use Hadrian to move from periodic testing to continuous, evidence-backed exposure reduction.

RECOGNISED BY LEADING ANALYSTS

Gartner GIGAOM

FROST & SULLIVAN

TRUSTED BY MARKET LEADERS

NBC · amadeus · McKESSON · BLINQX · CRÉDIT AGRICOLE · SHV ENERGY · ABN·AMRO · London Business School · RITUALS... · SIEMENS energy · LOTTOMATICA · LEROY MERLIN · WeatherTech · BIOLANDES · BLINQX · DAMEN · =EXACT · nedap