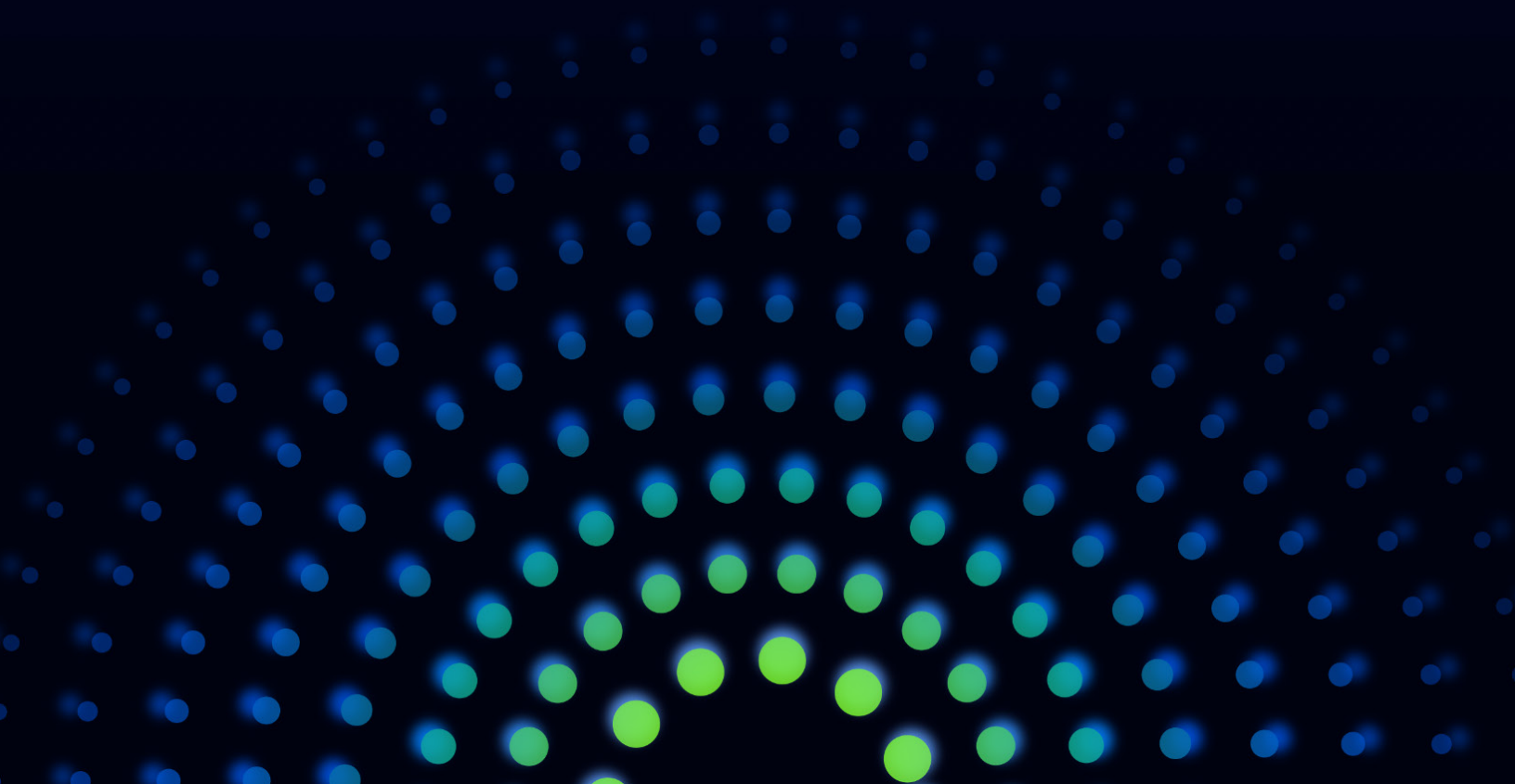




# Pentesting **Pulse Report**

How speed, AI, and quality are driving change  
in modern security testing





## The Satisfaction Gap and the AI Imperative

This Pentesting Pulse Report, based on a survey of 150 senior security professionals—including CISOs, security architects, engineers, and directors—uncovers a critical deficit in the pentesting market. While pentesting is overwhelmingly viewed as highly valuable for compliance and defense validation, satisfaction with current vendors is strikingly low. **Only 36% of security leaders say they are fully satisfied with their pentesting provider.**<sup>1</sup>

This disconnect is occurring while the industry faces a massive surge in vulnerabilities and an unprecedented need to secure new AI technologies. The findings show that security teams are urgently focused on **threat vulnerability management (76%) and securing AI adoption (50%)**.

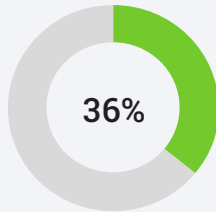
However, the slow, inconsistent, and often shallow nature of traditional services—evidenced by frustrations like the hurry-up-and-wait nature of **vendor rotation (28%)** and a **lack of expertise (17%)**—is creating a fundamental bottleneck. This points to a clear market requirement for a modern, agile security testing model, such as pentesting as a service (PTaaS), that can deliver the higher quality findings, specialized AI expertise, and the rapid scheduling needed to accelerate secure development at the speed of business.

---

<sup>1</sup>The survey of 150 U.S.-based respondents was conducted by Gatepoint Research in August 2025 through January 2026. Survey participants consisted of organizations not currently employing a PTaaS model for their penetration testing needs.

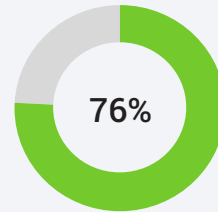
# Key Findings

## LOW VENDOR SATISFACTION



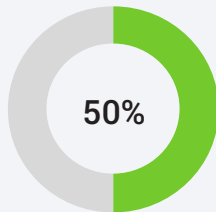
of respondents are fully satisfied with their current vendor

## TOP STRATEGIC GOAL



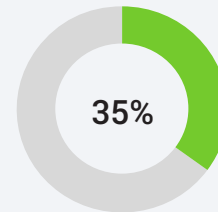
cite staying ahead of threats/vulnerabilities as a high-priority security goal

## THE AI IMPERATIVE



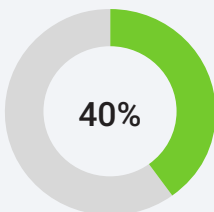
of leaders identified securing AI adoption within products as a key focus

## NEED FOR SPEED

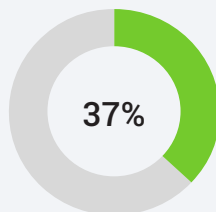


are motivated to switch vendors for the ability to schedule testing in days, not weeks

## QUALITY AND EXPERTISE

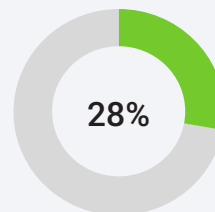


are motivated to switch vendors for higher quality testing

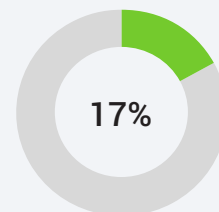


are motivated to switch vendors for expertise in AI pentesting

## OPERATIONAL FRICTION



express frustration with the operational drag of vendor rotation policies



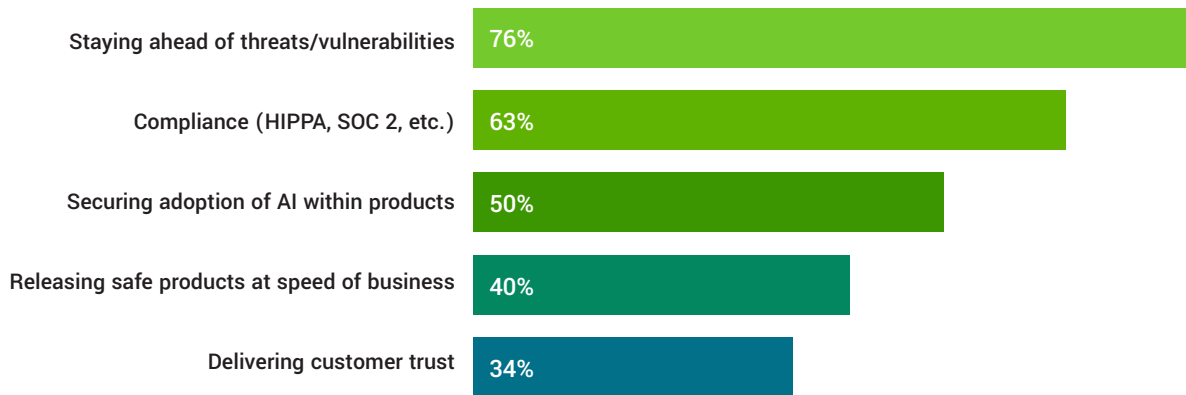
are concerned about failure to get pentests done on time

# The Evolving Mandate for Security Leaders

Security leaders are facing a dual-front war: maintaining foundational security and compliance while enabling the speed of business through AI innovation.

- **Threat and Compliance Drivers:** Staying ahead of threats (76%) and meeting regulatory mandates like HIPAA or SOC 2 (63%) remain the core high-priority goals.
- **The AI Challenge:** Half of respondents (50%) are prioritizing the secure adoption of AI. Plus, more than half (53%) report concerns with vulnerabilities from insecure code written by AI, a growing issue due to the rise of AI coding agents.
- **The Agility Imperative:** Releasing safe products at the speed of business (40%) requires a paradigm shift in security cadence.

## High-Priority Security Goals for 2026



### CISO PERSPECTIVE

“ Our survey confirms a truth we see every day: The era of the slow, shallow, check-the-box pentest is over. Our customers are building AI-driven products at the speed of business, but the market is still stuck in a paradigm that lacks specialized expertise. The low satisfaction score with vendors isn't a complaint—it's a clear market signal that security leaders need a scalable, high-quality partner that can integrate pentesting into the actual development lifecycle. This is precisely why we built the PTaaS model: to deliver expertise and insights at the speed of DevOps.

Andrew Obadiaru, CISO, Cobalt

# The State of Pentesting: Value, Usage, and the Quality Crisis

Pentesting remains a core security function, but the current delivery model is undergoing a crisis of faith in the quality of tests, expertise of testers, and real-time collaboration. Survey respondents report their biggest challenge is vendor rotation, which can exacerbate quality and speed issues due to onboarding and integrations.



## PENTESTING IS ESSENTIAL

The vast majority of the market (85%) views pentesting as a core security function, either as an invaluable defense validation (32%) or a key compliance facet (53%).

## The Crisis of Quality

Despite this high perceived value of pentesting, only 36% are fully satisfied with their vendors. The top reported challenges erode trust and efficiency.

### Vendor Rotation (28%)

Constant turnover of pentesting vendors creates an operational burden from onboarding, and setting up integrations and processes for communicating findings.

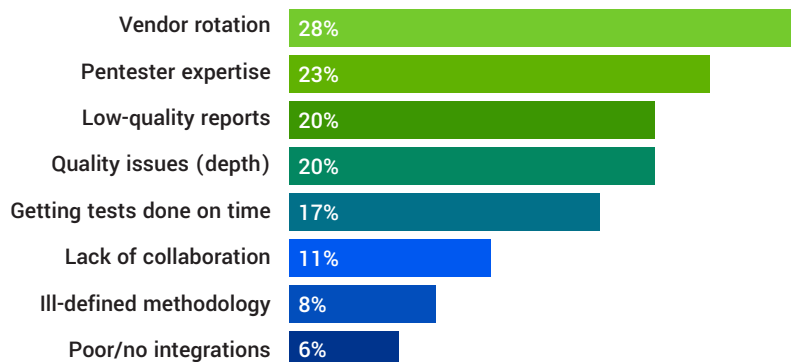
### Lack of Pentester Expertise (23%)

Generalist testers often lack the specialized knowledge for modern stacks. The expertise gap is especially apparent in small internal teams or boutique consultancies.

### Shallow Findings (20%)

A lack of depth in reports that don't contain explicit steps to reproduce findings, and details of how far a tester was able to infiltrate a system, make it difficult to remediate true risk. Automated scanners have this deficit in detailed reporting.

## Top Challenges with Current Pentest Programs



# The LLM Risk Paradox: High Anxiety, Low Readiness

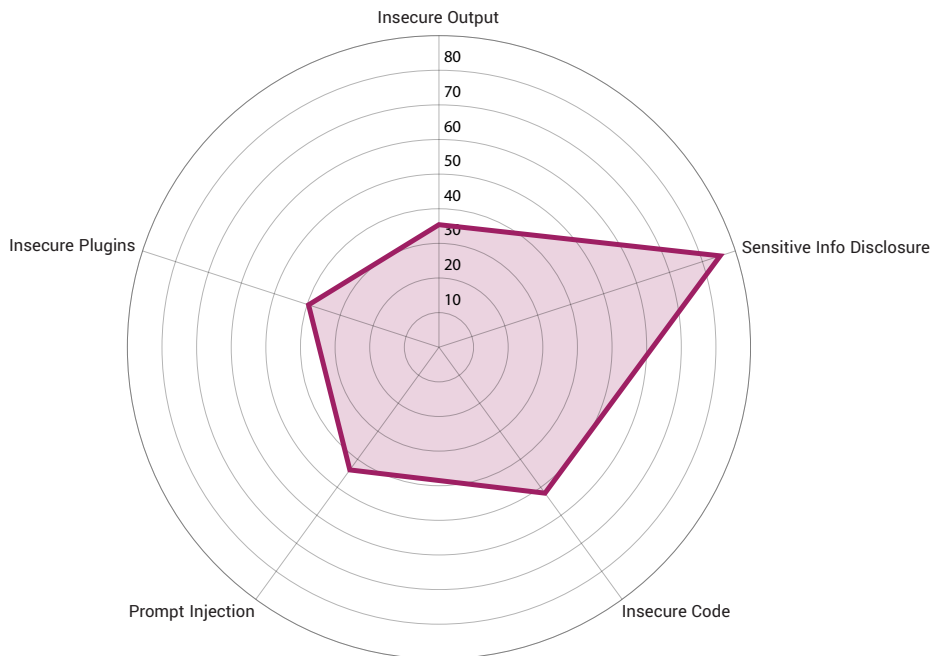
While the demand for AI is high, there is a profound gap between perceived risk and defensive capabilities. In our survey, 10% said they do not test AI/LLMs. However, according to the [Cobalt State of Pentesting Report](#), only one-third of organizations conduct regular testing of their AI applications. Even those doing testing are leaving many vulnerabilities unfixed.

## The Hierarchy of Concerns

Professional anxiety is focused heavily on data integrity. 85.4% of respondents identify Sensitive Information Disclosure as their primary fear regarding LLM usage.

- Sensitive Information Disclosure (**85.4%**)
- Vulnerabilities from Insecure Code Written by AI (**52.1%**)
- Prompt Injection (**43.8%**)
- Insecure Plugins/Access Control (**39.6%**)
- Insecure Output Handling (**35.4%**)

### Top Application Security Concerns: AI/LLMs



## The Readiness Gap

Only one-third (33%) of organizations conduct regular security assessments for their AI deployments. This is particularly dangerous given that 32% of all LLM pentest findings are classified as high or critical risk, according to Cobalt customer pentesting data.<sup>2</sup>

<sup>2</sup> Cobalt State of Pentesting Report, 2025.

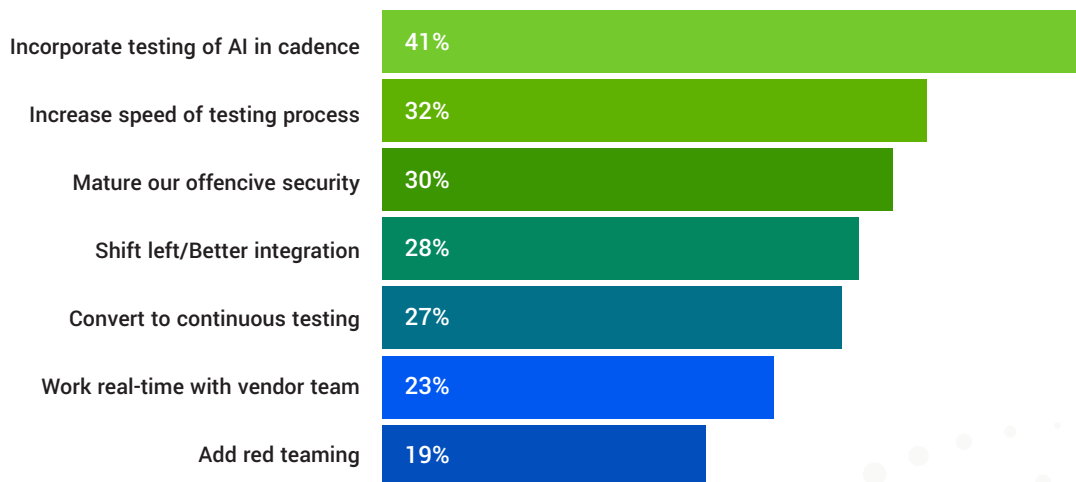
# The Agility Mandate: Redefining the Testing Cadence

To deliver secure products at the speed of business, security teams are moving away from rigid, legacy testing cycles and demanding a more integrated, responsive approach. Data from our survey reveals that the most critical strategic change desired by security leaders is **incorporating testing of AI into their regular cadence (41%)**. This shift is not merely about new technology; it's about maturing the entire offensive security posture to handle modern complexity.

Key strategic shifts identified include:

- **Speed and Maturity:** Beyond AI, 32% of respondents say their teams are focused on increasing the overall speed of the testing process, while 30% seek to fundamentally mature their offensive security capabilities.
- **Operational Integration:** There is a growing demand for shifting left, with 28% of leaders requiring better integration of pentesting into the software development process and 27% aiming to convert to a continuous testing model.
- **Real-Time Collaboration:** 23% of respondents identify the need to work in real time with their vendor's test team, moving away from static, "over-the-fence" reporting toward a collaborative partnership.

## Changes Needed to Deliver Secure Products Faster

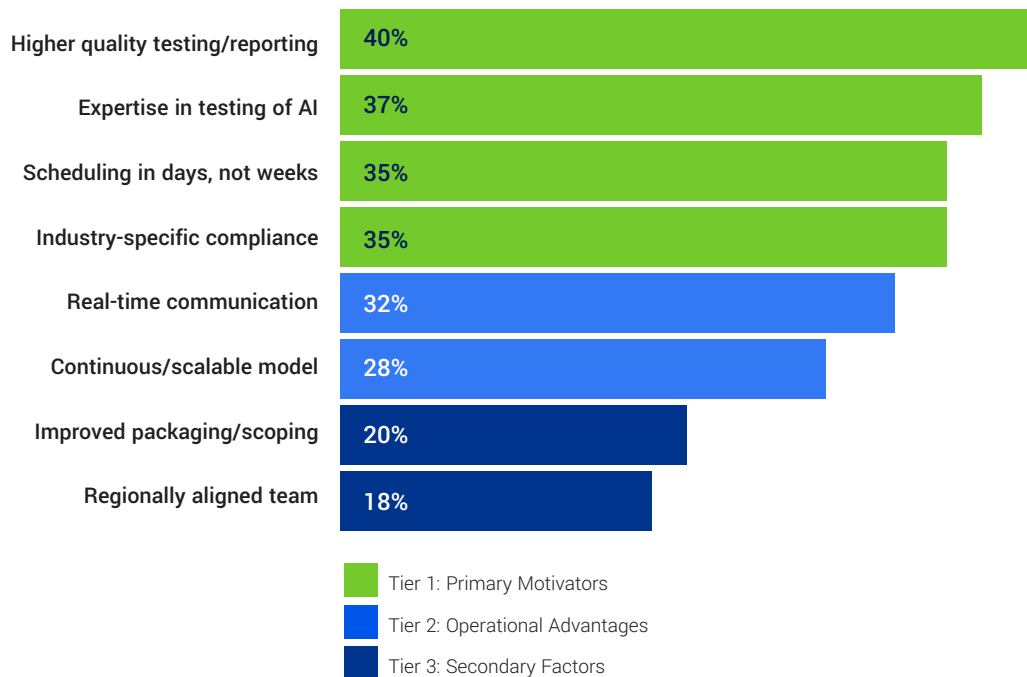


# The Modern Pen-testing Solution: Embracing PTaaS for the AI and Agility Era

Security stakeholders are actively seeking a more agile, high-quality model to match their innovation cycles. The satisfaction gap with pentesting providers is a clear market signal that the era of the slow, shallow, check-the-box pentest is over. These findings underscore that for 40% of security leaders, releasing safe products at business speed is a high priority goal—one that traditional vendor models simply cannot support.

- **Quality and Speed:** Increasing the speed of testing (32%) is among the top requested strategic changes. But respondents don't want speed at the price of quality. **40% say higher quality of pentesting is a top priority** that motivates them to evaluate new pentesting vendors.
- **The Demand for Expertise:** Specialized **expertise in testing of AI (37%)** is the second greatest motivator to evaluate new vendors.
- **Agility as a Differentiator:** Scheduling tests in **days, not weeks** is a critical requirement for 35% of leaders.

## Drivers to Evaluate a New Pentesting Vendor (3-Tier View)



# Recommendations for a Modern OffSec Program



## Demand Speed-of-Business Scheduling

Adopt PTaaS to ensure tests can be launched in days, not weeks, to avoid the release bottleneck.



## Verify Specialized AI Expertise

Address the demand for AI expertise by partnering with vendors who utilize human-led, creative testing to find complex AI flaws.



## Bridge the Remediation Gap

Move beyond fixing only “easy” vulnerabilities. Focus on high-risk AI findings, as currently only 21% of the highest risk LLM issues are resolved.



## Continuous Collaboration

Replace static reports with real-time communication between developers and testers to accelerate risk mitigation.



Discover how **human-led, AI-powered pentesting** can help you identify security gaps in your networks and applications.

[GET A DEMO](#)

## About Cobalt

Cobalt is the pioneer in penetration testing as a service (PTaaS) and a leader in human-led, AI-powered offensive security services. We are focused on combining talent and technology with speed, scalability, and expertise. Thousands of customers and hundreds of partners rely on the Cobalt Offensive Security Platform, along with 500+ trusted security experts, to find and fix vulnerabilities across their environments. By enabling faster pentest launches, real-time collaboration with pentesters, and seamless integration with remediation workflows, we help organizations identify critical issues and accelerate risk mitigation so they can operate fearlessly and innovate securely.