CASE STUDY

How Audiomob uses continuous pentesting from Cobalt to secure agentic development

The challenge

Audiomob helps brands reach tens of millions of engaged consumers daily through in-game and in-app advertising. Audiomob's global infrastructure enables advertisers to run audio campaigns without leaving their ecosystem, while orchestrating billions of real-time auctions per day.

Audiomob builds and ships code fast, with a constantly evolving attack surface. And with recent growth and well-earned industry recognition, they've gained the kind of attention that invites risk.

Like many companies, Audiomob has been using AI in software development for years. But within the last year, they made a more fundamental shift toward agentic engineering. This new development paradigm means their engineers increasingly direct AI agents, rather than writing code manually, so the development team can focus on planning, reviewing, and releasing.

Ville Laitinen, CTO at Audiomob, describes it as "a net-positive decision overall, but one that opens up new security threats and new things to consider." He adds: "It doesn't come without struggles."

Staying on the cutting edge of how software is built meant Audiomob needed a security partner who could keep pace with both their release velocity and evolving threat landscape.

> *"Cobalt is pentesting that fits how software is built."*
>
> Ville Laitinen
> *CTO, Audiomob*

Audiomob

ABOUT CUSTOMER

Audiomob is the global leader in in-game and in-app audio advertising. Audiomob helps brands reach tens of millions of engaged consumers, gamers, and app users on a daily basis. Their technology creates an unintrusive, uninterrupted experience in the app or the game for advertisers.

INDUSTRY
AdTech and Digital Advertising

SIZE
40+ employees

HEADQUARTERS
London, England

COBALT SERVICES
Web Application and API Pentesting

BY THE NUMBERS
Happy customer since 2023

The solution

Before Cobalt, Audiomob ran periodic security audits. They worked, but by the time a report landed it could already be outdated. Laitinen wanted a partner who could work continuously and evaluate their security posture the way an attacker would—because at Audiomob's scale, "even a small problem can have quite significant consequences."

They found that in Cobalt. The long-term partnership model meant knowledge accumulated over time, rather than starting from zero with each new engagement. Traditional audits, even when re-engaging the same pentesting vendor, might mean new testers who need to re-learn the architecture and re-evaluate the business logic.

With Cobalt, that knowledge carries forward. Ramp-up time for each new test is shorter, and Audiomob's ability to test on a flexible schedule every time they ship something new made the fit even stronger.

> *"Cobalt offers a lot of flexibility. We can test when we need to, for example when we roll something out."*
>
> Ville Laitinen
> *CTO, Audiomob*

That model stands in contrast to the point-in-time approach Audiomob left behind. As Laitinen says: "If your security shows up once per year as a PDF, it becomes almost a separate part of what you're doing—when it should be part of the daily work."

The results

The clearest measure of progress is what's no longer happening. Over three years of continuous testing, both the volume and severity of findings have decreased.

Laitinen credits much of that to the quality of testing that comes from testers who understand how Audiomob's systems actually work, a distinction that matters even more as agentic development opens up new and evolving security threats.

"We get more value from human testers, who can of course utilize AI in what they do, but have a more in-depth understanding of how our business works and how our systems work," he says. "That creates better quality tests than what you'd get from purely automated testing."

Testing depth has driven a broader cultural shift. Security thinking is now embedded in the engineering team from the start—a direct result of engineers seeing findings, fixing them, and internalizing the lessons continuously.

Early on, Audiomob presented every pentest at a company town hall. As findings became fewer and less severe, that stopped being necessary. Security has since moved into the engineering team's day-to-day work, with evidence of continuous testing shared through executive reporting, showing steadily improving results, and no critical findings.

Laitinen sums up the fit with Cobalt simply: "It's pentesting that fits how software is built, and how software actually works. It's not something separate, not something you bolt on, not something that creates friction. It supplements what we do. You get real testers, a platform that treats findings as engineering work instead of a document, which equals less ceremony, faster feedback loops, and the flexibility to test when it matters."

> *"With continuous testing, we can show that results are improving all the time, and that there are no critical findings."*
>
> Ville Laitinen
> *CTO, Audiomob*

To learn more about what Cobalt can do for your organization, visit cobalt.io/get-started

Cobalt

© 2026 Cobalt Labs, Inc. All Rights Reseved.