

How Personio built their offensive security program with Cobalt

THE CHALLENGE

As a leading HR software company experiencing rapid growth, Personio needed to adapt their security testing approach to match their fast-paced development cycle. After starting with annual pentests, it quickly became clear that a more agile approach was needed that could keep up with the ongoing cycle of new releases and updates. Point-in-time testing could leave substantial gaps where vulnerabilities might be introduced and remain undetected for extended periods, posing potential risks like data breaches and reputational damage. Personio's security team recognized the need to integrate testing earlier in the secure software development lifecycle (SSDLC).

THE SOLUTION

To address these concerns, Personio's security team began exploring how to embed pentesting earlier into their SSDLC. Personio partnered with Cobalt as one of their offensive security partners to enable continuous application testing throughout the development process, rather than only testing at major feature launches. Arnau Estebanell, Lead Security Engineer at Personio, explained: "With hundreds of deployments daily, our security controls need to be an enabler, not a blocker. Our offensive security program allows us to simulate real-world attacks early in the SSDLC, ensuring vulnerabilities are identified and fixed before they can be exploited by attackers – and at a lower cost."

Personio

ABOUT CUSTOMER

Personio empowers HR teams in small and mid-sized organizations to unlock the full potential of their employees, transforming the work experience for over a million people by offering an all-in-one intelligent platform.

INDUSTRY

Software Development: Human Resources

SIZE

1,800+ employees

HEADQUARTERS

Munich, Germany

COBALT SERVICES

Web Application Pentest, Mobile Application Pentest, AI and LLM Application Pentest, and Red Team

BY THE NUMBERS

15 pentests and 1 red team in 13 months

"We wanted to move beyond just 'checking the box' on pentesting. Cobalt enabled us to build a modern pentesting program with multiple assessments throughout the year. Their platform provides a central hub to orchestrate everything—from strategically planning tests to benchmarking our remediation speed against industry peers. We're now proactively managing risk through a continuous, data-driven security program."

ARNAU ESTEBANELL,
LEAD SECURITY ENGINEER, PERSONIO

THE OUTCOME

Over 13 months, Personio completed 15 penetration tests, including web, API, mobile, and LLM application assessments. They also conducted targeted engagements to evaluate the effectiveness of their security controls and detections.

Personio performed comprehensive assessments of their main SaaS platform, mobile application, and supporting APIs. To align with their development schedule, they conducted several agile pentests focused on new functionality—particularly changes that expanded the application's attack surface. For example, before launching their Personio AI Assistant, a dedicated LLM pentest provided valuable insights into AI vulnerabilities and mitigation strategies to address risks like model hallucinations.

Looking ahead, Personio has ambitious plans for its offensive security program. Personio will continue working closely with Cobalt to test earlier and more regularly, providing new insights into emerging threats. Arnau concludes: "Our goal is enabling Personio to move fast while staying secure. We're focused on balancing speed of delivery with robust security—allowing engineers to develop and release products quickly while keeping our customers' data protected, which remains our top priority. Cobalt's agile pentesting has been instrumental in helping us achieve this balance."

“

"With hundreds of deployments daily, our security controls need to be an enabler, not a blocker. Our offensive security program allows us to simulate real-world attacks early in the SSDLC, ensuring vulnerabilities are identified and fixed before they can be exploited by attackers—and at a lower cost."

ARNAU ESTEBANELL,
LEAD SECURITY ENGINEER, PERSONIO

”

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



WWW.COALT.IO

SAN FRANCISCO • LONDON • BERLIN

