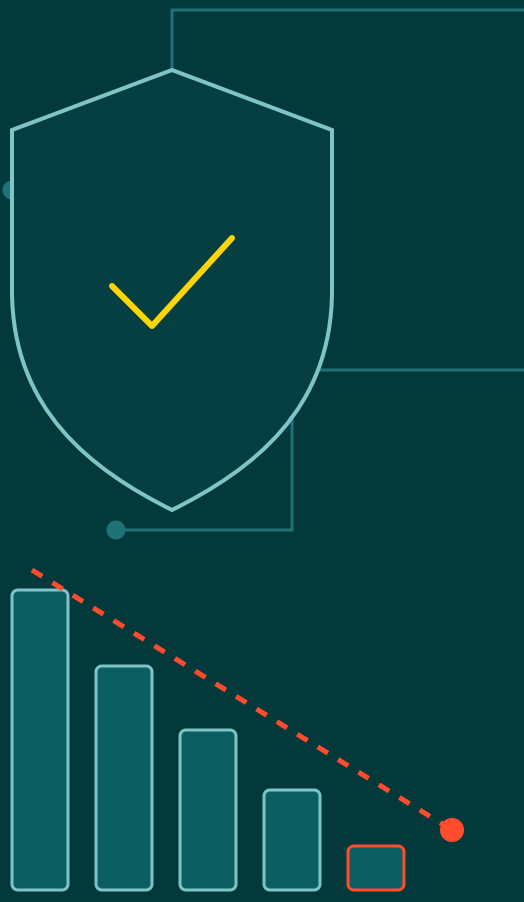
CASE STUDY

CS-2026-09

ioSENTRIX

Your Trusted Partner in Cybersecurity



APPLICATION SECURITY PROGRAMS

From 60,000+ ignored findings to zero open Critical or High in eight months

A gap analysis and roadmap turned scanner noise into a working AppSec program.

CLIENT
Large insurance company

SERVICE
Application security program

TIMELINE
Eight months to the result

RESULT
Zero Critical or High open

AT A GLANCE

CLIENT
Large insurance company

ESTATE
Hundreds of custom applications, many on-premises and legacy

SERVICE
Application security

SCOPE
Testing tools, AppSec processes, SDLC and developer training

START
A penetration test that exposed design and architecture flaws

TIMELINE
Eight months to the headline result, within a three-year roadmap

RESULT
Zero Critical or High open

DELIVERED BY
ioSENTRIX application security team

EXECUTIVE SUMMARY

Tools that cried wolf, a program that did not exist, and both now fixed

A large insurance company with hundreds of custom applications first hired ioSENTRIX for a penetration test. The issues we found pointed to design and architecture flaws, and to an application security program that was not working.

Its scanners had produced more than 60,000 open vulnerabilities that developers ignored, about 10% of them false positives. We ran a gap analysis, built a three-year roadmap and started a risk reduction campaign. More than 35% of the Critical findings were closed with platform-level fixes. Within eight months, no Critical or High vulnerabilities remained outstanding.

60K+	0	35%+
open vulnerabilities at the start	Critical or High outstanding after eight months	of Critical findings closed by platform-level fixes

The scanners were finding plenty. Nobody trusted them enough to act.

Details in this case study are anonymised and generalised. Methods that could harm other products are withheld.

© 2026 ioSENTRIX LLC

01 What we found

THEME · TOOLING FINDING 1

Scanners produced noise, not fixes

The company relied only on static and dynamic application security testing (SAST and DAST). Both were poorly configured, so false positives and legacy debt buried real issues, and developers ignored more than 60,000 reported vulnerabilities.

Business impact: real risks were lost in the noise, and the tools had lost the trust of the people meant to act on them.

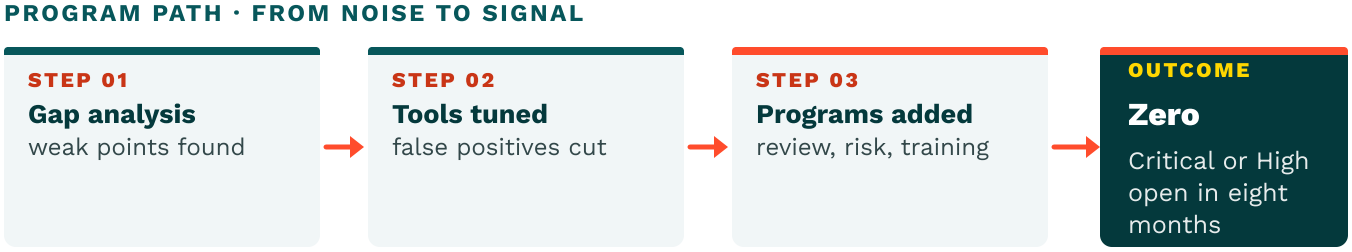
THEME · PROCESS FINDING 2

There was no program to act on results

There was no working vulnerability management or risk acceptance process. Exceptions in the governance system had fallen out of step with the scanners, leaving a build-up of outdated exceptions.

Business impact: nobody could say which risks had been accepted, by whom, or which needed fixing first.

Figure 1. The path from scanner noise to zero Critical or High



HOW WE FOUND IT

More tooling would have added more noise. The turnaround came from tuning what was there, building the processes around it and training developers on the organisation's own top risks.

© 2026 ioSENTRIX LLC

02 Results

Figure 2. What changed across the application estate

Outcome measured across the estate

AREA	BEFORE THE PROGRAM	AFTER EIGHT MONTHS
Open vulnerabilities	More than 60,000 reported issues that developers ignored	● No Critical or High vulnerabilities open
Tooling	Poorly configured SAST and DAST, buried in false positives	● Tuned SAST and DAST, about 10% of findings confirmed false positives; secret, IaC and dependency scanning added
Process	No vulnerability management or risk acceptance; stale exceptions	● Vulnerability management, risk acceptance and application security review programs
People	Security seen as noise by developers	● Training on the organisation's top 10 risks and reviews for high-risk apps

03 Lessons for security leaders

Tune before you buy

Untuned scanners produced 60,000+ findings nobody trusted. Fixing the configuration did more than a new tool would.

Finding 1

Build the program around the tools

Findings need owners, risk acceptance and review, or exceptions go stale and risk goes unseen.

Finding 2 · OWASP SAMM v2: Implementation and Verification business functions

Fix the platform, not each finding

More than 35% of the Critical findings were closed with platform-level fixes, such as OWASP ESAPI, instead of one by one.

Approach

ioSENTRIX

Drowning in scanner findings? See a sample program gap analysis or book a strategy session.

iosentrix.com/contact-us

contact@iosentrix.com

+1 (888) 958-0554

13800 Coppermine Rd, Suite 190
Herndon, VA 20171

CREST-accredited · ISO/IEC 27001 certified · SOC 2 Type 2 attested

© 2026 ioSENTRIX LLC. General information only. Client details anonymised.