CASE STUDY

Penetration Testing · Commercial

InterSec
Ignite . Inspire . Innovate

A Bug Bounty Program That Cut Critical Vulnerabilities by 75 Percent for a Wealth-Intelligence Platform

A FinTech platform with two decades of history needed to find the vulnerabilities that mattered without overspending. InterSec designed a bug bounty program that focused budget on verified, high-impact flaws and cut critical vulnerabilities by 75 percent.

CLIENT	PROFILE	STATUS
A wealth-intelligence FinTech platform	20+ years in market, data-driven insights for fundraising and business development	Completed

75%
Reduction in critical vulnerabilities

20+
Years operating in FinTech

0
Major exploits reaching operations

100%
Findings traced to verified root cause

MODEL	FOCUS	TRIAGE	REPORTING
Bug bounty over broad testing	Payment gateways, critical systems	Validated high-risk escalated at once	Technical and executive views

THE CHALLENGE

The company needed a cost-effective way to secure high-value financial data, and traditional testing was not pinpointing critical threats fast enough. The real problem was allocation: with finite resources, the firm could not spread security spend evenly across trivial and theoretical findings. It needed to concentrate on the issues that actually carried risk, while showing investors visible evidence of strong defenses.

THE APPROACH

InterSec designed a bug bounty program that incentivized ethical hackers to surface the most critical flaws first, so a limited budget went toward demonstrable risk reduction rather than volume. The design rested on three choices: a focused scope prioritizing business-critical systems such as payment gateways, rapid triage that escalated validated high-risk findings for immediate action, and transparent reporting for both technical teams and executives.

> **The vulnerabilities that matter most are rarely the ones a scanner flags first.**

THE SOLUTION IN PRACTICE

InterSec paired the bug bounty mechanics with close internal collaboration so each vulnerability was resolved quickly and accurately. Penetration testing and reporting verified the root cause of every finding and laid out step-by-step corrections rather than a raw list. The team guided the client's engineers through patch deployment and policy updates so fixes held, and kept researchers engaged for continuous coverage rather than a single point-in-time snapshot.

RESULTS & IMPACT

- ✓ Critical vulnerabilities fell by 75 percent by directing spend at the biggest risks.
- ✓ Major exploits were stopped before they could affect operations.
- ✓ The program gave the company a clear, demonstrable record of proactive, cost-effective security.
- ✓ Investors gained visible evidence of a credible security posture.

KEY TAKEAWAYS

Spend where the risk is.
A bug bounty model concentrates budget on verified, high-impact flaws instead of theoretical ones, which matters most when resources are finite.

Triage speed is a security control.
Escalating validated high-risk findings immediately is what turns a discovery into a closed gap.

Report to two audiences.
Technical teams need root cause and remediation steps. Executives and investors need the risk picture.

Point-in-time testing is not enough.
Keeping researchers engaged provides the continuous coverage a high-value financial target requires.

CAPABILITIES DEMONSTRATED

Bug Bounty Program Design · High-Impact Vulnerability Prioritization · Rapid Triage and Remediation · Cost-Effective Application Security · Stakeholder Reporting

Finite budget, high-value data: where do you point your testing?
InterSec designs bug bounty and penetration testing programs that find the flaws that matter first.

Let's talk →