SECURE CODERS.

# Accelerating Security for a Hyper-Growth Series B SaaS Startup

From Pre-Seed to Series B: A 4-Year Security Partnership

## Executive Summary

A high-velocity Sales/SaaS platform engaged SecureCoders before closing its seed round to pressure-test architecture and security controls. Four years later—and two funding rounds on—we serve as an always-on security partner delivering quarterly, feature-focused penetration tests, ad-hoc red-team exercises, and deep DevSecOps enablement. When a global incident-response firm was engaged for comparison, SecureCoders produced twice the actionable findings at less than half the cost, prompting the startup to consolidate all penetration-testing work with our team.

## Customer Profile

Industry

**Sales / SaaS**

Stage

**Series B (15 → 220 employees in 36 months)**

Tech Stack

**React front end • Clojure & Python micro-services on AWS (EKS) • Terraform-based IaC**

Compliance Drivers

**SOC 2 Type II, enterprise InfoSec questionnaires**

Engagement Duration

**4+ years (Pre-Seed to Series B)**

## Engagement Timeline

### Pre-Seed

Threat-model workshop & green-field architecture review

✓ Baseline controls embedded on day 0

### Seed → Series A

Annual full-stack penetration test; ad-hoc design reviews

✓ Closed critical auth bypass before public launch

### Series A → Series B

Quarterly pen tests mapped to sprint roadmaps; AWS config audit; spear-phishing & red-team drills

✓ 65% MTTR reduction; executives gained attack-surface visibility

### Series B

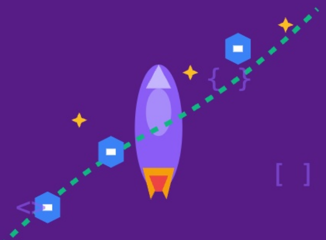
Embedded DevSecOps—SAST, SCA, container scanning, Terraform policy-as-code; CISO hiring support & SOC 2 prep

✓ Zero critical production vulns three straight quarters; SOC 2 Type II on first attempt

## The Challenge

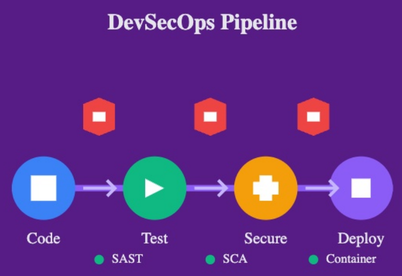
Rapid headcount growth, weekly feature releases, and a polyglot codebase (React, Clojure, Python) created a moving target for security. The startup needed:

- Continuous insight into new risks introduced every sprint
- Coverage beyond code—including AWS posture, CI/CD



pipelines, and social-engineering exposure

- A senior, on-call security team without the cost of full-time hires



### SecureCoders Approach

- **Shift-Left Pen Testing** – Quarterly assessments scheduled to coincide with major feature drops
- **Cloud & Infrastructure Audits** – IAM misconfigurations, Terraform drift detection
- **DevSecOps Pipeline Build-Out** – Integrated SAST, SCA, container scanning
- **Human-Centric Red Teaming** – Targeted phishing campaigns and SaaS abuse scenarios

## SecureCoders Services Delivered

- Quarterly Pen Tests aligned to sprint releases & new systems
- On-Demand Red Teaming (cloud assume-role abuse, targeted spear-phishing)
- DevSecOps Enablement—static analysis, container security, IaC remediation pipelines
- Executive Security Support—questionnaires, policy drafting, risk dashboards
- CISO Hiring Advisory—resume screening, interview panels, competency scorecards

## Key Outcomes

**-50%**
Cost vs. Big-4 Vendor

**0**
Critical Vulns in Prod (3 quarters)

**-65%**
Mean Time-to-Remediate

**100%**
SOC 2 Type II First Attempt

> *"SecureCoders feels like part of our engineering org—faster feedback, deeper findings, and real coaching for our team."*
>
> — VP Engineering, Series B Startup

## Recommendations & Next Steps

- Quarterly Purple-Team Drills aligning detection engineering with evolving threat intel
- Automated Cloud Drift Detection anchored to Terraform baselines
- Bug-Bounty Readiness Assessment ahead of planned public program launch
- Secure SDLC Metrics Dashboard tracking risk trends across repos & pipelines

## Why SecureCoders