

CASE STUDY

"At COE Security, we build, operate, and transfer world-class security solutions, empowering businesses with resilience and trust."

Joseph Henderson



COE SECURITY LLC

USA | BRAZIL | UAE | INDIA



CASE STUDY

FORTIFYING CODE, PROTECTING TRUST: APPLICATION SECURITY CONSULTING FOR A FINANCIAL SAAS PROVIDER



Measurable Impact Our Security in Numbers



- 1,500+ Global Engagements
- 95% Client Satisfaction
- 10+ Years of Cybersecurity Excellence
- 15K+ Critical Vulnerabilities Identified
- 1M+ Security Incidents Managed
- \$350M+ Costs Saved
- \$2.5B+ Transactions Secured
- 24/7/365 Threat Monitoring & Response
- Proactive Threat Hunting
- Cutting-Edge Security Technologies
- Dedicated Security Advisors
- Zero-Day Exploit Mitigation
- Incident Response Planning & Execution
- Security Awareness Training
- Customizable Security Solutions

**We're
Hiring!**

Client Profile

The client is a rapidly growing fintech company providing SaaS-based investment management tools to over 20,000 users across the United States. With a development team of 80 engineers and a portfolio of APIs and web applications handling sensitive financial data, the client needed to enhance application security amid growing customer demands, regulatory scrutiny, and multiple pen-test findings.

Challenges Faced

Key security concerns included:

- Insecure coding practices in CI/CD pipelines
- Lack of centralized visibility into application-layer vulnerabilities
- Inconsistent remediation of known OWASP Top 10 risks
- No formal AppSec training or secure SDLC integration

Solution

COE Security implemented a tailored Application Security Consulting Engagement, combining:

1. Static & Dynamic Code Analysis: Integrated SAST and DAST into CI/CD pipelines to catch issues early
2. Threat Modeling Workshops: Conducted scenario-based design threat assessments for core services
3. Secure Coding Training: Customized training for backend, frontend, and API developers
4. DevSecOps Strategy: Defined a shift-left security strategy with developer-owned security metrics



Compliance & Regulatory Mastery



- ISO 45001
- HIPAA & HITRUST
- NIST & NIST 800-171
- ISO 27001
- PCI DSS
- CMMC
- CIS Controls
- SOC 2
- CCPA & NYDFS
- EU CRA
- FedRAMP
- GDPR
- UK Cyber Essentials
- Essential Eight - Australia

**We're
Hiring!**

Securing the Software Lifecycle

- Integrated security tools into GitHub Actions for real-time scanning
- Reduced code vulnerabilities by 72% within three sprints
- Remediated all critical OWASP Top 10 issues within the first 60 days
- Enabled automated pull request checks for security gates
- Launched secure peer-review checklists for dev teams

Governance, Strategy, and Readiness

- Designed an AppSec roadmap with quarterly objectives and KPIs
- Defined ownership for security debt through threat severity-based SLAs
- Delivered an executive dashboard with security posture by repository
- Embedded security champions in each scrum team for decentralized accountability

COE Application Security Consulting Service Portfolio

- Secure SDLC Framework Design
- Static & Dynamic Application Testing
- Threat Modeling & Risk Analysis
- DevSecOps Pipeline Integration
- Application Penetration Testing
- Developer Security Training Programs
- API Security Assessments
- Code Review & Remediation Guidance
- Software Bill of Materials (SBOM) Creation
- AppSec Metrics, KPIs, and Reporting



Our Cybersecurity Arsenal: Beyond Protection- We Build Resilience



- Application Penetration Testing (Thick/Thin)
- Mobile Application Penetration Testing
- API Penetration Testing
- Network Penetration Testing
- Operational Technology Security Testing
- Cloud Penetration Testing
- AI & LLM Security Audit and Pen Testing
- Red Teaming & Social Engineering Services
- Product & Hardware Penetration Testing
- IoT Security
- Security Operations Center Services (24/7)
- Custom Security Services

Implementation Details

- Deployed GitHub-integrated SAST tools (CodeQL) and OWASP ZAP for staging environments
- Integrated AppSec plugins into Jenkins and GitLab runners
- Delivered role-based security training to over 80 developers
- Developed and delivered a secure coding guideline customized for internal frameworks
- Established reporting dashboards on Jira with remediation SLA tracking

Results Achieved

- 90% of high-risk vulnerabilities eliminated in production releases
- 3x faster remediation cycles via automated ticketing and CI/CD feedback
- Alignment with OWASP ASVS Level 2 for all external-facing apps
- Dev team maturity score increased from 2.5 to 4.2 (out of 5) on AppSec scale

Client Testimonial

“Partnering with COE Security transformed how we build software. Their pragmatic approach helped us align speed with security without disrupting our workflows. We’re now not just secure - we’re confident.”

**We're
Hiring!**



Industries We Protect with Cutting-Edge Security



- Financial Services
- Healthcare
- Retail
- E-commerce
- Government
- Cryptocurrency
- Blockchain Technology
- Automotive
- Transportation/Logistics
- Energy & Utilities
- Hospitality/Tourism
- Entertainment/Media
- Manufacturing
- Education
- Telecommunications
- HiTech & Information Technology

**We're
Hiring!**

COE Security LLC

COE Security is a leading cybersecurity services provider, offering comprehensive solutions to address the evolving threat landscape. We have a proven track record of helping organizations of all sizes mitigate risks, strengthen defenses, and recover from cyberattacks. Our team of experienced cybersecurity professionals possesses deep expertise in the latest technologies and best practices, enabling us to deliver tailored solutions that meet your unique security needs.

"Peace of mind in a world of cyber threats.
That's what we deliver."

Joseph Henderson

