CASE STUDY

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

Joseph Henderson

CASESTUDY

SECURE SOFTWARE DEVELOPMENT CONSULTING: BUILDING RESILIENT APPLICATIONS FROM THE GROUND UP

COE SECURITY LLC

USA | BRAZIL | UAE | INDIA

COE SECURITY

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

Client Profile

A fast-growing SaaS company developing cloud-based financial applications, requiring a security-first approach to software development to protect customer data, ensure regulatory compliance, and prevent cyber threats targeting their platform.

Challenges Faced

Modern software development presents significant security challenges, including:

- Code Vulnerabilities & Exploits Addressing security weaknesses in application code, including SQL injection, XSS, and insecure authentication mechanisms.
- Regulatory Compliance Ensuring software development aligns with GDPR, ISO 27001, PCI DSS, and other industry regulations.
- DevSecOps Integration Embedding security into CI/CD pipelines without disrupting rapid software delivery.
- Third-Party Dependencies & Open-Source Risks Managing security vulnerabilities in third-party libraries and APIs.

Solution

The organization partnered with COE Security to implement Secure Software Development Consulting, integrating robust security practices across the software development lifecycle (SDLC).

We're Hiring!

COE SECURITY

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

Secure Development Lifecycle Implementation

- Established a Secure SDLC framework integrating security best practices at every development phase.
- Conducted secure coding workshops for developers to identify and mitigate common vulnerabilities.
- Implemented static and dynamic application security testing (SAST & DAST) for early vulnerability detection.

Threat Modeling & Risk Assessment

- Performed application threat modeling to identify potential attack vectors before development.
- Assessed security risks related to business logic, API security, and user authentication workflows.
- Designed risk mitigation strategies to prevent common software security threats.

DevSecOps & CI/CD Security Integration

- Integrated automated security testing tools within CI/CD pipelines to catch vulnerabilities in real time.
- Implemented container security best practices for applications deployed in Kubernetes and cloud environments.
- Established security gates to prevent vulnerable code from reaching production.

We're Hiring!

COE SECURITY

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

Regulatory Compliance & Secure Coding Standards

- Aligned software development with PCI DSS, GDPR, ISO 27001, OWASP Top 10, and NIST secure coding guidelines.
- Conducted code reviews and penetration testing to validate compliance and identify security gaps.
- Developed compliance checklists for development teams to follow industry security standards.

Results

With COE Security's Secure Software Development Consulting, the organization achieved:

- Reduced Security Vulnerabilities Identified and remediated code flaws early, preventing exploits before production.
- Enhanced Compliance Readiness Ensured regulatory adherence to GDPR, PCI DSS, and security frameworks.
- Stronger DevSecOps Integration Automated security testing within CI/CD pipelines, improving software security without slowing down development.
- Improved Developer Security Awareness Trained engineering teams on secure coding practices, reducing human error-related vulnerabilities.
- Proactive Threat Mitigation Designed software with security in mind, minimizing attack surfaces and long-term risks.

We're Hiring!

COE SECURITY

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!

Client Testimonial

COE Security helped us integrate security into every stage of our software development. Their expertise in secure coding, threat modeling, and DevSecOps practices strengthened our applications and gave our customers confidence in our security posture.

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

Joseph Henderson

COE SECURITY