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

CASESTUDY

LLM DEVELOPER SURVEY: EMPOWERING SECURE AI INNOVATION THROUGH DEVELOPER INSIGHTS AND CONTINUOUS IMPROVEMENT.

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

A global financial services firm leveraged our six-phase LLM Developer Survey to benchmark secure-LLM readiness and close critical AI security gaps.

Challenges Faced

Development teams exhibited awareness gaps in key LLM threat vectors - prompt injection, data leakage, and model inversion - while toolchain fragmentation hindered consistent security controls. Only 25% of SDLC gates included AI-specific checks, leaving pipelines exposed to adversarial inputs and compliance risks under GDPR and PCI DSS. Without benchmarking data, leadership could not quantify maturity or prioritize remediation effectively.

Solution

We deployed a six-phase LLM Developer Survey combining quantitative analytics with qualitative insights to map developer practices against Secure SDLC standards. Phases included survey design, data-collection QA, statistical benchmarking versus NIST AI RMF and OWASP AMM, thematic mapping of open responses, actionable DevSecOps integration, and continuous iteration. This end-to-end methodology delivered prioritized remediation roadmaps, interactive dashboards, and CI/CD security hooks to harden prompt validation, adversarial testing, and governance gates.

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

Compliance Gap Assessment & Regulatory Alignment

We performed a comprehensive compliance gap assessment to benchmark the client’s LLM development practices against key regulations - GDPR, PCI DSS, HIPAA, and emerging AI-specific guidelines such as the EU AI Act and NIST AI RMF . Our analysis identified areas where data handling, consent management, and model transparency fell short of legal requirements, quantifying risk exposure across privacy, security, and governance domains . We mapped each finding to specific control objectives (e.g., data minimization, purpose limitation, audit logging) and provided a prioritized remediation matrix aligned with both internal policies and external mandates.

Risk Management & Due Diligence

We conducted legal and data-privacy due diligence - reviewing data-processing agreements, vendor contracts, and third-party AI service terms - to ensure full contractual and regulatory compliance . A risk register was developed to track identified gaps, assign ownership, and define mitigation timelines for high-impact items such as cross-border data transfers and automated decision-making disclosures . Integration of these compliance controls into the DevSecOps pipeline enabled real-time policy enforcement and audit-ready reporting, reducing legal exposure and strengthening data-privacy posture.

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

We're Hiring!

Implementation Details

We crafted a Secure SDLC-aligned questionnaire to capture developer roles, LLM use cases, and security practices - validating it through expert reviews and pilot tests. Responses were gathered via GitHub, Stack Overflow, and internal portals, with automated attention-checks and GDPR-compliant anonymization preserving data integrity. Quantitative analysis (frequency distributions, cross-tabulations, correlation tests) benchmarked teams against NIST AI RMF and OWASP AMM frameworks to generate an adoptability score. Thematic coding of open-ended feedback and expert interviews surfaced top concerns - prompt injection fears and toolchain gaps - and validated emerging threat vectors. Finally, we integrated findings into DevSecOps pipelines with SAST/DAST hooks, secure-coding libraries, and governance checkpoints for automated enforcement.

Results

With COE Security's LLM Developer Survey, the organization achieved:

- Closed 100% of critical prompt-injection vulnerabilities.
- Increased AI-specific SDLC gate coverage from 25% to 90%.
- Reduced remediation time by 60% through automated CI/CD security hooks.
- Boosted developer security awareness scores by 40% in follow-up surveys.

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's six-phase LLM Developer Survey rapidly revealed our security gaps, benchmarked us against NIST AI RMF and OWASP AMM, and delivered CI/CD-integrated fixes. In weeks, we closed all critical vulnerabilities and boosted developer security awareness by 40%, empowering us to scale LLM initiatives with confidence.

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

Joseph Henderson

COE SECURITY