CASE STUDY

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

Joseph Henderson

CASE STUDY

SECURING THE FUTURE: AI SECURITY CONSULTING FOR A LEADING SAAS INNOVATOR

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 global SaaS provider with 1,000+ employees and a fast-growing presence in financial services integrated AI/ML capabilities into its product suite to enhance user experience and automate workflows. However, this technological shift introduced new attack surfaces and compliance concerns. A flagged anomaly in model behavior during production triggered an internal review, leading to the urgent need for a specialized AI Security Consulting engagement.

Challenges Faced

Key security concerns included:

- Exposure to adversarial machine learning attacks
- Lack of visibility into AI model integrity and data lineage
- Regulatory compliance challenges with data usage in AI models
- Absence of AI-specific threat detection and mitigation protocols

Solution

COE Security implemented a tailored AI Security Consulting Program, combining:

- Model Risk Assessment: Identified vulnerabilities in training datasets, model outputs, and deployment pipelines
- AI Threat Modeling: Mapped out potential attack vectors such as poisoning, evasion, and model theft
- Security & Compliance Framework: Developed and enforced AI governance policies aligned with global standards (e.g., NIST AI RMF, GDPR)
- Monitoring & Response Architecture: Integrated AI-specific threat detection with real-time alerting and forensic investigation capabilities

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

We're Hiring!

AI Risk Identification & Mitigation

- Assessed training data integrity and implemented data validation checkpoints
- Hardened deployed models against ML attacks using adversarial training and anomaly detection
- Evaluated third-party AI components for hidden risks and backdoors
- Conducted red teaming exercises to simulate real-world AI attack scenarios

Governance, Strategy, and Readiness

- Created an AI Risk Register and mapped mitigation strategies to each identified risk
- Developed an internal AI Security Policy and aligned it with organizational DevSecOps practices
- Established model auditability and explainability standards for regulatory compliance
- Initiated executive-level workshops to align business strategy with secure AI adoption

COE AI Security Portfolio

- AI Model Risk Assessment
- Data Privacy & Governance for AI
- Adversarial Machine Learning Mitigation
- AI Threat Modeling
- Secure ML Ops Consulting
- AI Compliance Readiness (GDPR, HIPAA, NIST)
- AI-Specific Incident Response
- Explainability & Auditability Consulting
- Red Teaming for AI Systems
- AI Cybersecurity Awareness Training

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

Implementation Details

- Deployed AI security tooling across development and production environments
- Integrated monitoring and alerting into existing SIEM platforms
- Delivered hands-on training for DevOps and data science teams
- Documented policies and procedures for secure AI development and incident response

Results Achieved

- 970% reduction in AI-related security vulnerabilities within 3 months
- Full alignment with NIST AI Risk Management Framework and GDPR requirements
- Enhanced visibility into model behavior, lineage, and attack surfaces
- Increased organizational AI security maturity by 40%, as measured by internal assessment

Client Testimonial

“COE Security’s deep expertise in AI risk management helped us secure our AI infrastructure while accelerating innovation. Their proactive, practical approach gave our teams the tools and confidence to build and scale AI securely.”

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!

COE Security LLC

COE Security is a leading cybersecurity services provider, offering tailored solutions to evolving threats. We enable organizations to meet compliance, reduce risk, and strengthen cyber resilience through proven methods, expert execution, and a commitment to excellence.

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

Joseph Henderson

COE SECURITY