CASE STUDY

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

Joseph Henderson

CASE STUDY

STRENGTHENING TRUST IN INTELLIGENCE: AI SECURITY POSTURE ASSESSMENT FOR A GLOBAL 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

The client is a global Software-as-a-Service (SaaS) provider specializing in AI-driven customer experience platforms. With over 5,000 enterprise clients across 30+ countries and a development team of 800+ engineers, the client integrates AI into all facets of their operations—from automated chatbots to decision-making engines. As the adoption of AI grew, so did the associated risks. Concerns around adversarial ML, model poisoning, and data governance triggered the need for a comprehensive AI security posture assessment.

Challenges Faced

Key security concerns included:

- Lack of visibility into AI model risk and governance
- Potential vulnerabilities in model training pipelines
- Data integrity concerns in training datasets
- Absence of AI-specific security policies and controls

Solution

COE Security implemented a tailored AI Security Posture Assessment Engagement, combining:

1. Threat Modeling for AI Pipelines: Identified attack surfaces across ML lifecycle
2. Data Supply Chain Audit: Verified dataset provenance and manipulation risks
3. Model Risk Evaluation: Tested models against adversarial and evasion techniques
4. Governance Framework Mapping: Designed controls aligned with NIST AI RMF & ISO/IEC 23894

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

AI Risk Discovery and Mitigation Actions

- Mapped AI/ML architecture and workflows from data ingestion to model deployment
- Conducted red team simulations targeting ML attack vectors (e.g., model inversion, poisoning)
- Discovered data drift and implemented monitoring with alert thresholds
- Reviewed open-source dependencies in AI toolkits (TensorFlow, PyTorch, etc.)
- Built risk registers and proposed mitigation measures for all identified gaps

Governance, Controls, and Strategic Recommendations

- Established an AI governance committee and policy charter
- Integrated secure model lifecycle checkpoints in CI/CD
- Developed explainability and bias mitigation controls
- Defined risk rating and audit tracking methodology for AI components

COE AI Security Posture Assessment Service Portfolio

- AI/ML Risk Assessments
- Threat Modeling for AI Pipelines
- Adversarial Testing & Model Hardening
- Data Supply Chain Integrity Audits
- AI Governance Frameworks (ISO 23894, NIST AI RMF)
- Secure MLOps Enablement
- Bias & Fairness Testing
- Explainability Validation (XAI)
- AI Audit Trail Automation
- Developer Training in AI Secure Engineering

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

Implementation Details

- Deployed model evaluation sandbox and adversarial testing tools
- Integrated model integrity scans into existing CI/CD pipeline
- Delivered tailored training sessions to 60+ ML engineers and data scientists
- Produced detailed AI threat models and process documentation
- Set up quarterly AI security reporting aligned with board KPIs

Results Achieved

- 70% improvement in AI model governance maturity (baseline to benchmark)
- Reduced AI model attack surface by 60% via patching and architectural hardening
- Established AI audit trails covering 100% of core ML workflows
- Increased stakeholder trust and regulatory alignment with ISO 23894 draft

Client Testimonial

“COE Security gave us clarity on AI risk where we had none. Their depth in both cybersecurity and machine learning helped us future-proof our models and meet emerging governance expectations.”

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 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

COE SECURITY