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

SAFEGUARDING ARTIFICIAL INTELLIGENCE SYSTEMS IN A RAPIDLY EVOLVING LANDSCAPE

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 cutting-edge technology company specializing in artificial intelligence (AI) solutions for various industries, including healthcare, finance, and manufacturing.

Challenges Faced

As AI technology evolved, the company faced new cybersecurity risks, from adversarial attacks on machine learning models to unauthorized data access and system manipulation. The client needed a robust strategy to secure its AI infrastructure and maintain client trust in its products and services.

- Protecting Machine Learning Models Defending against adversarial attacks and model manipulation that could lead to inaccurate predictions and compromised systems
- Securing Sensitive Data Ensuring that AI models and datasets are secure, preventing data leaks and unauthorized access to proprietary algorithms
- Compliance with AI Regulations Adhering to evolving global regulations around AI, including data privacy, algorithm transparency, and ethical use of AI
- Incident Response and Monitoring Implementing systems to detect, respond to, and recover from cyber threats targeting AI systems

Solution

The AI company partnered with COE Security to design a customized security framework that addressed the unique vulnerabilities of AI and machine learning systems.

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 Model Protection and Integrity

- Implemented adversarial training techniques to improve AI system resilience against adversarial attacks
- Applied robust encryption methods for both training data and machine learning models to prevent unauthorized access and tampering
- Developed anomaly detection algorithms to identify potential data poisoning and manipulation of AI models

Data Security and Privacy Enhancement

- Strengthened data access controls to protect sensitive datasets used for training AI models, ensuring compliance with GDPR and other data privacy laws
- Integrated homomorphic encryption for secure data processing, allowing computations on encrypted data without compromising privacy
- Introduced secure APIs and authentication mechanisms for data sharing and collaboration between different AI systems and third-party providers

AI System Monitoring and Threat Detection

- Deployed continuous monitoring systems to detect unusual activities and potential vulnerabilities in AI workflows
- Established real-time incident response capabilities to address potential breaches or system failures promptly
- Integrated machine learning-based security tools to automatically detect and mitigate threats against AI systems

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 and Ethical AI Standards

- Assisted in aligning AI practices with global regulations like GDPR, CCPA, and emerging AI-specific frameworks
- Developed ethical AI guidelines for model transparency, accountability, and fairness, ensuring unbiased decision-making in AI applications
- Provided ongoing compliance audits and support to maintain regulatory adherence and mitigate legal risks

Results

With COE Security's AI security solutions, the technology company achieved:

- Resilient AI Models Protected machine learning systems from adversarial attacks and ensured reliable, accurate outputs
- Enhanced Data Security Secured sensitive datasets and training data while maintaining compliance with global privacy regulations
- Continuous Monitoring and Threat Detection Identified and mitigated security threats proactively, ensuring the safety of AI infrastructure
- Regulatory Adherence Met the stringent ethical and legal standards of AI, promoting trust and compliance with clients and stakeholders

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 provided us with the specialized expertise we needed to protect our AI systems and ensure that our technology remains secure and compliant with global standards. Their proactive approach to security has given us peace of mind, knowing our AI models and data are safe.

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

Joseph Henderson

COE SECURITY