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

AI SECURITY POSTURE ASSESSMENT: SAFEGUARDING AI-DRIVEN SYSTEMS AGAINST EMERGING THREATS

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 technology company leveraging artificial intelligence (AI) and machine learning (ML) for predictive analytics, automation, and data processing across finance, healthcare, and manufacturing sectors. The organization needed to evaluate and strengthen the security of its AI models, algorithms, and data pipelines.

Challenges Faced

As AI adoption increased, the organization encountered several cybersecurity and compliance challenges:

- AI Model Vulnerabilities & Adversarial Attacks Risk of model poisoning, data manipulation, and adversarial inputs affecting AI decision-making.
- Data Privacy & Compliance Risks Required adherence to GDPR, ISO 27001, NIST AI RMF, and sector-specific regulations.
- Lack of AI-Specific Security Controls Needed a structured security framework to mitigate AI system vulnerabilities.

Solution

The organization partnered with COE Security to conduct an AI Security Posture Assessment, ensuring AI-driven technologies remained secure, resilient, and compliant with evolving regulations.

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

Comprehensive AI Security Risk Assessment

- Evaluated AI models for adversarial robustness, bias detection, and data integrity.
- Assessed the security of AI training datasets to prevent poisoning and data leakage risks.
- Conducted red team exercises to simulate real-world AI cyber threats and attack scenarios.

AI Security Framework & Risk Mitigation Strategies

- Implemented secure AI development lifecycle (SAI-DevSecOps) best practices.
- Strengthened AI model explainability and transparency to mitigate unintended biases and security risks.
- Established AI governance policies aligning with emerging AI security regulations and industry standards.

Regulatory Compliance & Ethical AI Governance

- Ensured AI compliance with GDPR, ISO 27001, NIST AI Risk Management Framework, and global AI security guidelines.
- Developed policies for responsible AI use, ethical AI deployment, and model accountability.
- Provided documentation and audit readiness support for AI security governance.

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!

Threat Monitoring & AI System Resilience

- Integrated AI threat detection mechanisms to identify malicious inputs and adversarial activities.
- Established continuous AI model security monitoring for emerging threats.
- Provided incident response strategies for AI-driven cybersecurity incidents.

Results

With COE Security's AI Security Posture Assessment, the organization achieved:

- Enhanced AI Model Security Identified and mitigated adversarial risks, securing AI decision-making processes.
- Regulatory Compliance Assurance Ensured AI systems met GDPR, ISO 27001, and AI security framework requirements.
- Secure AI Development & Deployment Integrated security best practices across the AI lifecycle.
- Stronger AI Governance & Risk Management Implemented robust policies for AI ethics, privacy, and security.
- Continuous Threat Protection Established proactive monitoring and incident response for AI security threats.

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 AI security expertise helped us fortify our AI models against adversarial attacks and data breaches. Their structured approach to AI governance, compliance, and risk mitigation has been instrumental in securing our AI-driven applications. Highly recommended!

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

Joseph Henderson

COE SECURITY