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 ADOPTABILITY SECURITY REVIEW FOR A LEADING SAAS PROVIDER

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 over 1,000 employees and a rapidly expanding customer base in financial services. The client had begun integrating AI and ML technologies across their platform to enhance automation and decision-making capabilities. However, the lack of secure AI development practices and growing concerns over model integrity, data privacy, and compliance triggered the need for a comprehensive AI security review.

Challenges Faced

Key security concerns included:

- Exposure to adversarial attacks on deployed ML models
- Use of unvetted third-party AI components
- Lack of visibility into AI risk across development and production environments
- Limited readiness among DevOps and data science teams regarding AI threat mitigation

Solution

COE Security implemented a tailored AI Security Posture Enhancement Program, combining:

- AI Threat Modeling: Identified vulnerabilities across AI/ML pipelines and model lifecycles
- Data & Model Risk Assessment: Audited datasets and trained models for integrity and bias
- Toolchain Hardening: Secured MLOps environments and CI/CD pipelines
- Capability Building: Conducted workshops to upskill development and security teams

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 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 & Readiness Framework

- Developed AI-specific security policies and operational procedures
- Established secure model lifecycle management practices
- Integrated AI risk metrics into the enterprise governance dashboard
- Defined escalation and response protocols for AI-related incidents

COE Security's AI Assurance Service Portfolio

- AI Security Readiness Assessment
- Secure MLOps Integration
- Model Threat Simulation (Red Teaming)
- Bias & Fairness Auditing
- Third-Party AI Component Vetting
- Secure Model Deployment Playbooks
- AI-Specific Incident Response Planning
- Training for AI Developers & Security Teams
- AI Risk Monitoring & Dashboarding

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 AI security tools across dev, test, and production environments
- Integrated monitoring and alerting into existing SIEM platforms
- Delivered hands-on training for DevOps and data science teams
- Documented secure AI development policies and incident handling procedures

Results Achieved

- 30% reduction in exposure to AI-related security risks
- Integrated risk monitoring across 100% of AI model deployments
- Achieved compliance alignment with emerging AI governance standards
- Increased AI security maturity score by 40% within six months

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