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 INNOVATION ACROSS BORDERS: AI GEO-ADOPTION SECURITY REVIEW

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 multinational technology conglomerate with over 10,000 employees, spanning AI innovation hubs across North America, Europe, and Southeast Asia. With rapid AI-driven product rollouts and global expansion, the client sought to assess and fortify their security posture concerning region-specific data privacy laws, AI model integrity, and geo-specific threat landscapes.

Challenges Faced

Key security concerns included:

- Fragmented compliance strategies across geographies (GDPR, HIPAA, APPI, etc.)
- AI model exposure to region-specific adversarial threats
- Insufficient controls on AI/ML data pipelines
- Lack of centralized visibility into geo-adoption risk profiles

Solution

COE Security implemented a tailored AI Geo-Adoption Security Review Program, combining:

1. Geo Threat Surface Mapping: Mapped AI workloads against regional cyber threat trends
2. Compliance Gap Analysis: Benchmarked AI usage against applicable data sovereignty laws
3. Model Security Assessment: Evaluated exposure to poisoning, evasion, and inference attacks
4. Unified Risk Dashboard: Built a centralized governance interface to track security and compliance status across global deployments

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!

Risk Reduction Across Intelligent Systems

- Assessed 12 production AI models across 5 countries
- Mapped region-specific attack vectors impacting AI performance and compliance
- Hardened ML inference pipelines using differential privacy and model watermarking
- Introduced automated red-teaming exercises simulating geo-specific threat actors
- Reduced time-to-detect model tampering by 70%

Governance and Strategic Oversight

- Implemented an AI Governance Framework aligned with ISO/IEC 42001 and NIST AI RMF
- Established regional security champions for AI deployment units
- Centralized policy controls for data residency, model update processes, and audit logging
- Developed a federated incident response playbook for AI-specific threats

COE AI Geo-Adoption Security Review Service Portfolio

- AI/ML Threat Modeling
- Geo-Adoption Security Strategy
- Model Poisoning & Evasion Risk Assessment
- Secure AI/ML Pipeline Architecture
- AI Data Provenance & Integrity Checks
- Regulatory Alignment for AI Systems
- AI-SOC Integration
- Federated Privacy Enforcement
- Continuous Red Teaming for AI Systems
- Global Compliance Reporting Dashboard

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

- Integrated AI model telemetry with SIEM and XDR platforms
- Conducted red team simulation training for regional teams
- Delivered region-specific compliance documentation and SOPs
- Enabled monthly board-level security and compliance briefings

Results Achieved

- 85% reduction in AI security blind spots across regions
- Achieved compliance alignment with GDPR, CCPA, and PDPA simultaneously
- Implemented 24/7 model monitoring, reducing MTTD from 3 weeks to 2 days
- Elevated AI security maturity score from Level 1 to Level 4 in 6 months

Client Testimonial

“COE Security brought clarity and control to our most complex global AI deployments. Their proactive, geo-aware approach made security a business enabler—not a bottleneck.”

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