CASE STUDY

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

Joseph Henderson

CASE STUDY

FORTIFYING INTELLIGENCE: AI RUNTIME DEFENSE ANALYSIS FOR A CLOUD-NATIVE SAAS LEADER

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 mid-sized, cloud-native SaaS enterprise delivering AI-driven analytics platforms to financial institutions. With a global customer base spanning 12 countries and a development workforce of 400+ engineers, the organization relies heavily on real-time AI decision engines embedded in its core services. After experiencing anomalies and unexplained behavioral shifts in production AI models, the client approached COE Security to evaluate and strengthen their runtime AI defense capabilities.

Challenges Faced

Key security concerns included:

- Undetected adversarial inference attacks at runtime
- Lack of monitoring for abnormal AI behavior or drift
- Vulnerabilities in AI microservices communicating over APIs
- No existing response playbook for AI-specific threats

Solution

COE Security implemented a tailored AI Runtime Defense Analysis Program, combining:

1. Behavioral Baseline Modeling: Established expected behavior signatures for AI model outputs
2. Runtime Threat Hunting: Deployed detection mechanisms for adversarial patterns and payloads
3. Security Observability for AI Pipelines: Integrated telemetry for inference layer monitoring
4. Incident Response Tuning for AI Events: Built AI-specific detection rules and response logic

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!

Runtime Risk Identification and Remediation

- Monitored AI models in production across multiple services using model observability tools
- Detected multiple drift events and one targeted adversarial input incident
- Implemented dynamic input validation at API endpoints before model invocation
- Introduced anomaly alerts tied to model confidence score deviations
- Secured inter-service communication with encrypted AI payloads

Governance and Readiness for AI-Driven Threats

- Updated SOC playbooks to include AI threat classifications and response procedures
- Integrated runtime model insights into SIEM for continuous detection
- Designed dashboards for tracking AI model health, drift, and confidence integrity
- Recommended use of eBPF-based telemetry for AI inference nodes

COE AI Runtime Defense Analysis Service Portfolio

- AI/ML Runtime Defense Analysis
- Adversarial Input Detection Systems
- Real-time Drift Monitoring and Alerting
- Secure AI Model API Gateways
- AI-specific SOC Playbooks
- Secure AI Containerization (Kubernetes, Docker)
- AI Incident Forensics
- Production Model Health Dashboards
- Runtime Telemetry Injection
- Model Confidence Deviation Detection

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 telemetry agents on AI inference servers for runtime monitoring
- Integrated AI anomaly metrics into existing Prometheus-Grafana stack
- Conducted red-team simulation to test runtime defense effectiveness
- Delivered technical documentation with AI threat models and response guides
- Provided monthly executive reports with model drift and threat summaries

Results Achieved

- 100% runtime model visibility achieved across inference endpoints
- 3 critical AI vulnerabilities identified and remediated
- Enabled 24x7 AI threat monitoring integrated into SIEM
- SOC team's AI incident response capability improved by 65% (based on drill performance)

Client Testimonial

"COE Security helped us gain real-time visibility into our AI systems and stop threats before they impacted customer trust. Their AI-aware approach to cybersecurity gave us a clear edge."

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