INSPYR SOLUTIONS

Comprehensive AI Security Assessment & Implementation

Challenge

A major retailer operating throughout the U.S. sought to enhance the company's AI capabilities by granting their AI system access to proprietary information. The goal was to give the AI enough information to answer questions and produce materials in a context tailored to the business, but this required access to a large body of sensitive data. Recognizing the significant risks associated with exposing internal data to an AI system, especially one powered by large language models (LLMs), the client sought comprehensive security expertise.

The client needed a partner who could address:

- Potential **novel security risks** when exposing data to AI/LLMs.
- **Safeguarding data** against misuse, exposure, or loss.
- Expert **implementation** of security measures.
- Updating **security policies** to reflect new standards.
- Remediating **security vulnerabilities**.
- Educating the internal team to **take over security and prepare for the future**.

The client had already experienced success working with INSPYR Solutions on several AI initiatives, so they turned to their trusted partner once again to secure business-critical information while unlocking deeper insights.

Solution

INSPYR Solutions engaged our leading industry expert in AI security

Because the client was proactive, they were able to safeguard their data before experiencing any significant issues.

as a foundational member of the team deployed for the three-phase project. The team took a systematic approach to establish a deep understanding of the overall enterprise and the associated risks it was facing. This ensured that every aspect of security would be evaluated, giving INSPYR Solutions a comprehensive understanding of the targeted improvements required, from the procedural level down to day-to-day operations.

Phase I: Discovery and Assessment – INSPYR Solutions examined the client's systems, including the AI and LLM operations and existing security policies. The team identified gaps in the security landscape and created a roadmap for remediation through updated policies, procedures, and practices.

Phase II: Policy Updates and Execution – During this phase, INSPYR Solutions performed the initial work laid out in the roadmap, which included updating legacy security policies and procedures, creating new ones where appropriate, and implementing best practices for AI security.

Phase III: Rollout and Training – At this point, INSPYR Solutions rolled out changes to secure the AI environment. This phase also included training the client's security team so they could move forward with the new policies and procedures, giving them the tools they needed to keep the company's data secure in the future. INSPYR Solutions also trained software engineers, data engineers, infrastructure engineers, and end users on how to implement best practices at their associated levels because a security-aware company culture must exist at all levels to succeed.

Solution highlights include:

- **Deep assessment** and understanding of the company's current security posture.
- Creation of a **roadmap** to a more secure system.
- Updating **security policies** and **procedures** and creating new ones where needed.
- Mitigation of **existing security risks**.
- Implementation of new **security policies, procedures, and practices**.
- **Training** at all organizational levels.

Outcome

By the end of the project, the company had a more secure environment and the client's team had a better understanding of AI security at all levels of the organization. By updating the methodologies and shifting the company culture to be more aware of security concerns around AI/LLMs, the client could move forward with new initiatives and gain better insight into operations with current business data.

The AI security initiative yielded key benefits, including:

- **Comprehensive training** at all levels ensured that both those building the technology and those using it are informed about the security implications of AI.
- New and improved **policies, procedures, and practices** provide guardrails for working with AI.

- Existing **security gaps were addressed**, safeguarding data against breaches and unauthorized access.
- The client now has a **clear roadmap** and ongoing processes to continuously **assess and improve** their AI security posture.

Because the client was proactive about security surrounding the implementation of AI, they were able to benefit from the expertise of a trusted AI security partner and safeguard their data before experiencing any significant issues.

With better awareness of how these technologies work and where data could be at risk, the client is better equipped to protect sensitive, proprietary information while still benefitting from the many applications of AI.

After multiple successful AI projects, INSPYR Solutions now leads the company's overall AI initiatives, providing thought leadership and expertise in this fast-growing field.

Client Profile

The client is a major retailer both online and across its many physical locations in the U.S. The company serves a diverse customer base by fulfilling a wide variety of needs no matter where customers are. This Fortune 500 business is known for providing great value to consumers through quality products, excellent service, and low prices.

Technologies Supported

Popular AI Features: Artificial Intelligence, Machine Learning, Generative AI, Computer Vision, Facial Recognition, Object Detection

About INSPYR Solutions

Technology is our focus and quality is our commitment. As a national expert in delivering flexible technology and talent solutions, we strategically align industry and technical expertise with our clients' business objectives and cultural needs. Our solutions are tailored to each client and include a wide variety of professional services, project, and talent solutions. By always striving for excellence and focusing on the human aspect of our business, we work seamlessly with our talent and clients to match the right solutions to the right opportunities. Learn more about us at inspyrsolutions.com.