EINPRESSWIRE

Thoropass partners with DynamoFL to pioneer application pentests for GenAI systems

The companies are driving innovation in how AI is tested and applied in compliance and security

Thoropass compliance and audit solution

NEW YORK, NEW YORK, USA, March 5, 2024 /EINPresswire.com/ -- Thoropass continues to lead the compliance industry forward by announcing a partnership with DynamoFL that will advance the protection of sensitive data related to AI LLMs. Already a leader in infosec compliance and audits, Thoropass is extending its pentesting offering with DynamoFL, a venture-backed startup founded out of MIT that's focused on deploying compliant-ready enterprise Gen AI.

> “The Thoropass-DynamoFL partnership enhances the capabilities of our Web LLM pentest by leveraging DynamoFL's DynamoEval platform to identify PII extraction and data extraction vulnerabilities.”
>
> *Sam Li*

Thoropass, who has provided compliance automation software and auditing solutions since its founding five years ago, also provides proprietary pentesting to align with compliance as the first step to customers' larger security goals. As customers increasingly use and train artificial intelligence large language models (AI LLMs), the need for compliance has become urgent.

DynamoFL is the leader in Privacy Preserving Generative AI and specializes in technology that evaluates and fortifies LLM-based systems for privacy, security, and compliance risks. In targeting both open and closed-source LLMs, DynamoFL's DynamoEval platform can test for reverse-engineering of training data, privacy attacks on membership inference and model inversion, memorization vulnerabilities, hallucinations, and 15 additional use cases. The net result is a safe and trustworthy LLM that is better aligned with the expectations of compliance regulations such as GDPR, CCPA, and other emerging global AI regulations and security standards.

In a Web LLM penetration test, Thoropass performs a simulated attack to identify and exploit vulnerabilities often seen in LLM applications, highlighting their potential impact, ease of exploitation, and prevalence in real-world applications. Examples of vulnerabilities include prompt injections, data leakage, inadequate sandboxing, and unauthorized code execution, among others.

“The Thoropass-DynamoFL partnership enhances the capabilities of our Web LLM pentest by leveraging DynamoFL's DynamoEval platform to identify PII extraction and data extraction vulnerabilities,” said Thoropass CEO and Co-Founder Sam Li. “Together we’re able to offer a secure and scalable solution for companies looking to make safe investments in their AI LLMs.”

With technology and services paired together, Thoropass and DynamoFL will be able to deliver pentesting that is accessible to companies of any size looking to innovate while being mindful of evolving worldwide AI regulations.

"Together with Thoropass, we are excited to introduce our joint solution ensuring that enterprise Gen AI applications undergo meticulous testing against privacy, security, and compliance risks, particularly when deploying to customer-facing production use cases. With our combined expertise, enterprises of all sizes can confidently deploy their Gen AI solutions, knowing they meet the highest standards of integrity and reliability,” said DynamoFL CEO and Co-Founder Vaikkunth Mugunthan.

Customers can take advantage of this partnership in their AI pentesting efforts right away. Thoropass and DynamoFL will continue to adapt this solution to new cases. The companies will also work toward releasing a compliance framework addressing AI usage and regulations by the end of the year.

For more information about Thoropass, DynamoFL, and pentesting, visit
http://info.thoropass.com/ai-pentesting

ABOUT THOROPASS:
At Thoropass, we’re compliance experts so you don’t have to be. Pairing easy AI-infused software that’s always getting smarter with expert guidance and continuous monitoring, we integrate into your processes to prepare customers to pass any audit, every year, while saving time and resources. Hundreds of growing companies use Thoropass’s compliance and audit solution, expert services, in-house auditors, and partner ecosystem to get and stay compliant over the lifetime of their business. We offer SOC 2, ISO 27001, HITRUST, GDPR, HIPAA, PCI DSS, and other infosec and privacy frameworks.

ABOUT DYNAMOFL:
DynamoFL develops privacy-preserving tools and techniques for enabling compliant-ready Gen AI. Our customers, in all industries, leverage our product suite across: DynamoEval: Evaluate your existing closed or open-source LLMs for privacy, security, hallucination, and reliability risks;

DynamoEnhance: Deploy privacy-preserving fine-tuning and advanced LLM development tools to mitigate identified risks; and DynamoGuard: Enable real-time moderation of internally or 3rd party hosted LLMs, configured for your organization’s specific AI policies.

Chris Gerben
Thoropass
chris.gerben@thoropass.com
Visit us on social media:
LinkedIn