Microsoft, NVIDIA, Google and many other major technology companies form the Coalition for Secure AI (CoSAI)

With the rapid development of artificial intelligence technology, new challenges and potential risks are also appearing, requiring an effective management mechanism on a global scale.

That's why the Coalition for Secure AI (CoSAI), a new watchdog and support agency in the field of artificial intelligence, was officially announced today at the Aspen Security Forum. . CoSAI's founding team are the world's leading technology companies in the AI ??field, including Google, IBM, Intel, Microsoft, NVIDIA and PayPal. In addition, the list of 'co-sponsored' brands are also big names: Amazon, Anthropic, Cisco, Chainguard, Cohere, GenLab, OpenAI and Wiz.

The CoSAI initiative was created primarily to provide basic to detailed guidance through open source methods, frameworks and standardized tools, empowering developers to create innovative systems. Secure-by-Design AI system is safe and user-friendly. CoSAI will especially focus on developing, integrating, deploying and safely operating AI systems, minimizing risks such as model theft, data poisoning, and command injection attacks (AI Prompt Injection).), abuse and inference attacks.

Similar to other open source community projects, CoSAI will establish a Project Governing Board to promote and manage the overall technical program. In parallel with that, there will be a Technical Steering Committee consisting of leading AI experts from different organizations and businesses around the world participating in monitoring each work process.

In the first phase, CoSAI will focus on the following issues:

1. **Secure software supply chains for AI systems** : enhance component tracking and provenance to secure AI applications.
2. **Building preventative solutions for the changing cybersecurity landscape** : solving development and integration challenges in AI and classical systems.
3. **AI security governance** : develop best practices and risk assessment frameworks for AI security.

Speaking about the initiative to establish CoSAI, CoSAI Board Co-Chair David LaBianca, said:

The founding of CoSAI stems from the need to democratize the knowledge and advances needed for the safe integration and deployment of AI. This will be possible through collaboration between leading companies, experts and academia.

CoSAI's mission is to create an open source approach to AI security - a critical step toward building trust and promoting responsible development in the rapidly expanding AI industry. By addressing the fragmented nature of current security measures and providing standardized guidance, CoSAI aims to empower developers and organizations to create more secure AI systems .