Introducing the Coalition for Secure AI, an OASIS Open Project

CoSAI's Founding Sponsors Include Google, IBM, Intel, Microsoft, NVIDIA, PayPal, Amazon, Anthropic, Cisco, Chainguard, Cohere, GenLab, OpenAI, and Wiz.

BOSTON, MA, USA, July 18, 2024 /EINPresswire.com/ -- The Coalition for Secure AI (CoSAI) was announced today at the Aspen Security Forum. Hosted by the OASIS global standards body, CoSAI is an open-source initiative designed to give all practitioners and developers the guidance and tools they need to create Secure-by Design AI systems. CoSAI will foster a collaborative ecosystem to share open-source methodologies, standardized frameworks, and tools.

CoSAI brings together a diverse range of stakeholders, including industry leaders, academics, and other experts, to address the fragmented landscape of AI security.

- CoSAI's founding Premier Sponsors are Google, IBM, Intel, Microsoft, NVIDIA, and PayPal. Additional founding Sponsors include Amazon, Anthropic, Cisco, Chainguard, Cohere, GenLab, OpenAI, and Wiz.

- CoSAI is an initiative to enhance trust and security in AI use and deployment.

- CoSAI's scope includes securely building, integrating, deploying, and operating AI systems, focusing on mitigating risks such as model theft, data poisoning, prompt injection, scaled abuse, and inference attacks.

- The project aims to develop comprehensive security measures that address AI systems' classical and unique risks.

- CoSAI is an open-source community led by a Project Governing Board, which advances and manages its overall technical agenda, and a Technical Steering Committee of AI experts from academia and industry who will oversee its workstreams.

The Need for CoSAI

Artificial intelligence (AI) is rapidly transforming our world and holds immense potential to solve complex problems. To ensure trust in AI and drive responsible development, it is critical to develop and share methodologies that keep security at the forefront, identify and mitigate potential vulnerabilities in AI systems, and lead to the creation of systems that are Secure-by-Design.

Currently, securing AI and AI applications and services is a fragmented endeavor. Developers grapple with a patchwork of guidelines and standards which are often inconsistent and siloed. Assessing and mitigating AI-specific and prevalent risks without clear best practices and standardized approaches is a significant challenge for even the most experienced organizations.

With the support of industry leaders and experts, CoSAI is poised to make significant strides in establishing standardized practices that enhance AI security and build trust among stakeholders globally.

“CoSAI's establishment was rooted in the necessity of democratizing the knowledge and advancements essential for the secure integration and deployment of AI," said David LaBianca, Google, CoSAI Governing Board co-chair. "With the help of OASIS Open, we’re looking forward to continuing this work and collaboration among leading companies, experts, and academia."

"We are committed to collaborating with organizations at the forefront of responsible and secure AI technology. Our goal is to eliminate redundancy and amplify our collective impact through key partnerships that focus on critical topics," said Omar Santos, Cisco, CoSAI Governing Board co-chair. "At CoSAI, we will harness our combined expertise and resources to fast-track the development of robust AI security standards and practices that will benefit the entire industry.”

Initial Work

To start, CoSAI will form three workstreams, with plans to add more over time:

- Software supply chain security for AI systems: enhancing composition and provenance tracking to secure AI applications.

- Preparing defenders for a changing cybersecurity landscape: addressing investments and integration challenges in AI and classical systems.

- AI security governance: developing best practices and risk assessment frameworks for AI security.

Participation

Everyone is welcome to contribute technically as part of the CoSAI open-source community. OASIS welcomes additional sponsorship support from companies involved in this space. Contact join@oasis-open.org for more information.

See a complete list of CoSAI Founding Sponsors' quotes here.

Additional Information
CoSAI charter

About OASIS
One of the most respected, nonprofit open source and open standards bodies in the world, OASIS advances the fair, transparent development of open source software and standards through the power of global collaboration and community. OASIS is the home for worldwide standards in AI, cybersecurity, supply chain, IoT, privacy, and other technologies. Many OASIS standards go on to be ratified by de jure bodies and referenced in international policies and government procurement. www.oasis-open.org

Media inquiries
communications@oasis-open.org

Carol Geyer
OASIS
+1 941-284-0403
carol.geyer@oasis-open.org
Visit us on social media:
LinkedIn
X
Facebook
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/728099287