Google Donates Secure AI Framework (SAIF) Data to Coalition for Secure AI, Advancing Industry-Wide AI Security Standards

OASIS Open Project Accelerates Collaborative Development of Open Source AI Security Tools and Best Practices

CoSAI SAIF Donation from Google

BOSTON, MA, UNITED STATES, September 16, 2025 / EINPresswire.com/ -- OASIS Open, the international open source and standards consortium, announced that Google has donated data from its Secure AI Framework (SAIF) to the Coalition for Secure AI (CoSAI), an OASIS Open Project. The contribution includes the Coalition for Secure AI Risk Map (CoSAI-RM), now available as part of CoSAI Tooling. The CoSAI-RM is a framework for identifying, analyzing, and mitigating security risks in AI systems, providing a structured map of the AI security landscape and a common language to address vulnerabilities that traditional software security practices often miss. CoSAI will continuously update, develop, and expand the Risk Map to address emerging threats and evolving security challenges in AI systems.

This contribution strengthens CoSAI's mission to enhance trust and security in AI development and deployment, directly supporting its four Workstreams: Software Supply Chain Security, Preparing Defenders for a Changing Cybersecurity Landscape, AI Security Risk Governance, and Secure Design Patterns for Agentic Systems.

Heather Adkins, Google, VP Security Engineering, said, "Google developed SAIF to address the unique security challenges that emerge as AI systems become more sophisticated and widely deployed. By contributing this framework to CoSAI, Google is ensuring that organizations of all sizes can access the same security principles and practices that we use to protect our own AI systems."

SAIF provides a comprehensive approach to AI security that spans the entire AI development lifecycle, including practical tools such as the SAIF Risk Assessment, which helps organizations

identify and mitigate AI-specific vulnerabilities, including data poisoning, prompt injection, and model source tampering.

"Google's SAIF contribution represents the kind of industry leadership that makes CoSAI successful by bringing proven security frameworks developed at scale directly into the hands of the global AI community," said J.R. Rao, IBM, Co-Chair of the CoSAI Technical Steering Committee (TSC). "This donation will significantly accelerate our workstreams, especially on AI Security Risk Governance, and provide immediate, practical value to organizations working to secure their AI deployments. It's a perfect example of how open collaboration can transform innovative research into accessible tools that benefit everyone."

Get Involved

CoSAI now includes more than 40 industry partners working collaboratively to address AI security challenges. Its Premier Sponsors, including EY, Google, IBM, Microsoft, NVIDIA, Palo Alto Networks, PayPal, Snyk, Trend Micro, and Zscaler, are leading the way in advancing secure AI practices. CoSAI's work is also grounded in the support of its Founding Sponsors: Amazon, Anthropic, Cisco, Cohere, GenLab, Google, IBM, Intel, Microsoft, NVIDIA, OpenAI, PayPal, and Wiz.

Technical contributors, researchers, and organizations are welcome to participate in its open source community and support its ongoing work. OASIS welcomes additional sponsorship support from companies involved in this space. Contact join@oasis-open.org for more information.

About CoSAI

The Coalition for Secure AI (CoSAI) is a global, multi-stakeholder initiative dedicated to advancing the security of AI systems. CoSAI brings together experts from industry, government, and academia to develop practical guidance, promote secure-by-design practices, and close critical gaps in AI system defense. Through its workstreams and open collaboration model, CoSAI supports the responsible development and deployment of AI technologies worldwide.

CoSAI operates under OASIS Open, an international standards and open-source consortium.
www.coalitionforsecureai.org

About OASIS Open

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, emergency management, identity, IoT, cybersecurity, blockchain, privacy, cryptography, cloud computing, urban mobility, and other content 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

Jane Harnad
OASIS Open
email us here
