Coalition for Secure AI Welcomes Palo Alto Networks and Snyk, Advances AI Security with New Publication and Workstream

Whitepaper on AI Supply Chain Risks and Agentic Systems Workstream Strengthen the Coalition's Impact on Secure AI Development

BOSTON, MA, UNITED STATES, June 26, 2025 /EINPresswire.com/ -- The Coalition for Secure AI (CoSAI), an OASIS Open Project dedicated to advancing AI security, proudly welcomes Palo Alto Networks and Snyk as Premier Sponsors. Their commitment reinforces CoSAI's rapidly expanding network of 45 partner organizations united in the mission to advance secure and trustworthy AI. This growth comes as CoSAI deepens its technical leadership with the release of a whitepaper focused on securing the AI software supply chain and the launch of a dedicated workstream on secure agentic system design, addressing the security implications of increasingly autonomous AI systems.

Expanding Industry Support

"Securing AI is one of the most urgent challenges facing the industry today," said Sam Kaplan, Assistant General Counsel for Public Policy & Government Affairs, Palo Alto Networks. "By joining CoSAI, Palo Alto Networks is proud to support open collaboration that empowers developers to embed security from the start."

Manoj Nair, Chief Innovation Officer, Snyk, added, "As AI transforms the cybersecurity landscape, proactive security standards are essential. Snyk is excited to contribute to CoSAI's growing efforts to develop practical, open tools for safer AI adoption."

Palo Alto Networks and Snyk join CoSAI's distinguished group of Premier Sponsors - including EY, Google, IBM, Microsoft, NVIDIA, PayPal, Protect AI, Trend Micro, and Zscaler - united in accelerating the development of secure and responsible AI across industries.

New Landscape Paper: Addressing Security Risks in the AI Supply Chain

CoSAI's first landscape paper, Establish Risks and Controls for the AI Supply Chain, explored further in our blog post, was developed through cross-sector collaboration to help teams integrate security at every stage of the AI system lifecycle, from design to deployment. Published by CoSAI's Workstream 1: Software Supply Chain Security for AI Systems, the paper examines the unique supply chain security risks of AI systems, focusing on data, infrastructure, applications, and models, and highlights the need for specialized safeguards beyond traditional security practices. It also outlines key vulnerabilities, roles across stakeholder groups, and evaluates existing frameworks like SAIF, MITRE ATLAS, and OWASP AI Exchange to identify gaps and guide a more resilient, secure AI development lifecycle.

"This landscape paper is a significant step forward in AI security, offering comprehensive risk overview and practical protection strategies," said Matt Maloney, Manager of Technical Staff at Cohere and CoSAI Workstream 1 Lead. "It's an important resource mapping supply chain risks and highlighting where traditional controls fall short," added Andre Elizondo, Principal Solutions Engineer at Wiz and CoSAI Workstream 1 Lead. Both emphasized the paper's evolution alongside emerging AI agent technologies.

Introducing a New Workstream on Secure Agentic System Design

To address the growing need for secure-by-design approaches to autonomous AI, CoSAI has launched Workstream 4: Secure Design Patterns for Agentic Systems (https://github.com/cosai-oasis/ws4-secure-design-agentic-systems). This new track focuses on developing security models and architectural guidance for agentic systems, including updates to AI threat modeling, secure infrastructure design, and cross-system integration.

The addition of Workstream 4 complements CoSAI's three existing workstreams:

Workstream 1: Software Supply Chain Security for AI Systems
Workstream 2: Preparing Defenders for a Changing Cybersecurity Landscape
Workstream 3: AI Security Risk Governance

"The launch of a workstream focused on Secure Agentic System Design reinforces CoSAI's commitment to addressing the growing complexity of AI-driven autonomous systems," said Workstream 4 Leads Sarah Novotny, Independent Consultant, and Ian Molloy, Department Head, Securing AI, IBM Research. "As agentic systems become more capable and pervasive, it becomes critical to ensure they are built on a foundation of security, transparency, and accountability."

Get Involved
CoSAI welcomes technical contributors, researchers, and organizations 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
CoSAI is an open ecosystem of AI and security experts from industry-leading organizations dedicated to sharing best practices for secure AI deployment and collaborating on AI security research and product development. CoSAI operates under OASIS Open, the 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
