Coalition for Secure AI Releases Two Actionable Frameworks for AI Model Signing and Incident Response

OASIS Open Project Delivers Practical Tools to Build Trust and Defend AI Systems at Scale

BOSTON, MA, UNITED STATES, November 18, 2025 / EINPresswire.com/ -- OASIS Open, the international open source and standards consortium, announced the release of two critical publications advancing AI security practices from the Coalition for Secure AI (CoSAI), an OASIS Open Project. These new resources provide practical frameworks to help organizations strengthen the security and trustworthiness of their AI systems. CoSAI's Software Supply Chain Security for AI Systems Workstream released "Signing ML Artifacts: Building towards tamper-proof ML metadata records" and the Preparing Defenders for a Changing Cybersecurity Landscape Workstream published "AI Incident Response Framework V1.0." Together, these frameworks address key aspects of the full lifecycle of AI assurance, from preventing tampering before deployment to responding effectively when systems are attacked.

Model Signing: Building Trust in AI Supply Chains

Workstream 1's publication, "Signing ML Artifacts," addresses one of the most pressing challenges in AI deployment: verifying the authenticity and integrity of AI models before integrating them into mission-critical systems. As AI becomes woven into critical business processes, the question is no longer whether to implement model signing, but how quickly organizations can move to adopt it. Workstream 1's guidance offers both the technical depth and implementation roadmap needed to accelerate adoption while ensuring interoperability across

the AI ecosystem and maintaining the security, trust, and compliance their businesses demand.

"Model signing delivers tangible business value: reduced security risk, streamlined compliance, and increased stakeholder trust. This framework gives enterprises the tools to confidently deploy AI while maintaining visibility and control over their most valuable ML assets throughout their entire lifecycle," said the Workstream 1 Leads, Andre Elizondo of Wiz, Matt Maloney of Cohere, and Jay White of Microsoft.

The publication introduces a staged maturity model designed to help organizations adopt model signing effectively, beginning with establishing basic artifact integrity through digital signatures, ensuring that models can be verified against unauthorized changes. It then advances to incorporating signature chaining and lineage, which create clear provenance trails and enable traceability across the entire AI supply chain. Finally, it integrates structured attestations and policy controls to support comprehensive AI governance frameworks that align with organizational security and compliance requirements.

AI Incident Response: Preparing Defenders for Evolving Threats

AI systems face unique threats including data poisoning, model theft, prompt injection, and inference attacks that traditional incident response frameworks aren't designed to handle. Workstream 2's "AI Incident Response Framework V1.0" equips security practitioners with comprehensive, AI-specific guidance to detect, contain, and remediate these emerging threats.

"AI adoption is reshaping enterprise security, and operationalizing incident response with rapidly changing technology presents new challenges," said Vinay Bansal of Cisco and Josiah Hagen of Trend Micro, CoSAI's Workstream 2 Leads. "This framework presents incident examples over common AI use cases and provides playbooks specific to new risks in AI systems, helping organizations move from theory to practice."

The framework complements existing guidance by addressing capabilities and gaps unique to AI. It helps defenders minimize the impact of AI exploitation while maintaining auditability, resiliency, and rapid recovery, even against sophisticated threats. The guide also tackles the complexities of agentic AI architectures, emphasizing forensic investigation and providing concrete steps to prioritize security investments, scale mitigation strategies, implement layered defenses, and navigate AI governance challenges.

Industry Collaboration and Impact

Together, these publications – developed from the collaborative efforts of CoSAI's more than 40 industry partners, including Premier Sponsors EY, Google, IBM, Microsoft, NVIDIA, Palo Alto Networks, PayPal, Snyk, Trend Micro, and Zscaler – build on and reinforce CoSAI's broader initiatives, including the recent Strategic Update, the donation of Google's Secure AI Framework (SAIF), and the Principles for Secure-by-Design Agentic Systems.

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

Mary Beth Minto
OASIS Open
email us here
Visit us on social media:
LinkedIn