Cisco Donates Project CodeGuard to Coalition for Secure AI

Framework Strengthens Secure-by-Default Practices in AI Coding Workflows

BOSTON, MA, UNITED STATES, February 9, 2026 /EINPresswire.com/ -- OASIS Open, the global open source and standards consortium, announced that Cisco has donated Project CodeGuard, an AI model-agnostic security coding agent skills framework and ruleset, to the Coalition for Secure AI (CoSAI), an OASIS Open Project. The framework embeds security best practices directly into AI-assisted software development, helping to prevent vulnerabilities introduced by AI coding agents and generating more secure code automatically.

Addressing AI Coding Security Risks

As AI coding agents rapidly transform software engineering, the speed and efficiency they provide can inadvertently introduce security risks, including skipped input validation, hardcoded secrets, weak cryptography, unsafe functions, and missing authentication or authorization checks.

Project CodeGuard addresses these challenges across the full development lifecycle: guiding design before code is written, preventing vulnerabilities during code generation, and supporting AI-assisted code review afterward.

"Project CodeGuard represents Cisco's commitment to advancing security at the scale and speed of AI," said Anthony Grieco, Chief Security & Trust Officer, Cisco. "While this is a major step forward, we are just getting started. By contributing this framework to CoSAI's open ecosystem, together, we are building security into AI coding from the start. Making these practices freely

available will elevate security across the industry and protect the software that powers our collective world."

For more details on the donation and technical capabilities, read more in the blog post, Cisco's Donation of Project CodeGuard to CoSAI: A New Chapter in Securing AI-Generated Code.

"Project CodeGuard exemplifies CoSAI's vision of bringing together industry expertise to solve real-world AI security challenges," said David LaBianca, CoSAI Co-Chair, Google. "This framework empowers developers with the tools they need to create secure code. Through our open collaboration model, we'll work with the community to expand these capabilities and drive adoption across the industry, advancing our shared mission of making AI systems more secure and trustworthy."

Comprehensive Security Coverage

Project CodeGuard provides multi-layered security coverage across several domains: cryptography, input validation, authentication, authorization, access control, supply chain security, cloud and platform security, and data protection. This approach ensures that security considerations are woven throughout the development process.

The framework integrates seamlessly with AI assistants including Cursor, GitHub Copilot, Windsurf, Claude Code, and others, using a unified markdown format that translates easily to integrated development environment (IDE)-specific formats.

Development Through Special Interest Group

The ongoing development and extension of Project CodeGuard will be conducted through a dedicated Special Interest Group (SIG) within CoSAI's AI Security Risk Governance Workstream. The collaborative structure will enable technical contributors, researchers, and organizations to work together on expanding the framework's capabilities and driving its adoption across the AI development community.

Get Involved

CoSAI brings together more than 40 industry partners to advance secure AI, share guidance for deployment, and collaborate on AI security research and tools. Its Premier Sponsors, including EY, Google, IBM, Meta, Microsoft, NVIDIA, PayPal, Snyk, Trend Micro, and Zscaler, are leading the way in advancing secure AI initiatives. 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
+1 781-425-5073
email us here