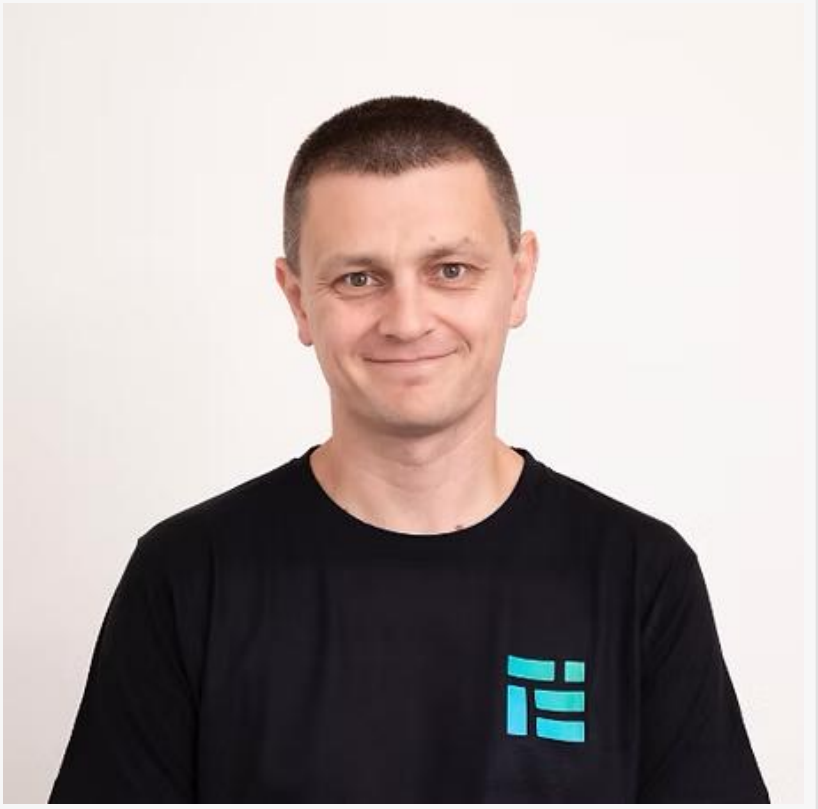
Commugen Unveils AI Risk Management Platform to Tackle “Shadow AI” Threat

Built for CISOs, Commugen AI Risk Management Solution delivers real-time visibility, regulatory mapping, and automated guardrails for AI-assisted development.


Vladimir Tyomin, CTO of Commugen

TEL AVIV, ISRAEL, August 14, 2025 /EINPresswire.com/ -- Commugen launches AI risk management platform to help CISOs detect, govern, and secure unsanctioned AI use in software development environments.

Generative AI developer tools such as GitHub Copilot, CodeWhisperer, ChatGPT, and Claude are transforming the speed and agility of software delivery. But beneath the innovation lies a growing and often invisible threat. Vladimir Tyomin, Chief Technology Officer at Cyber GRC leader Commugen, is warning CISOs and cyber governance leaders that “Shadow AI” is already embedded deep within developer workflows, bypassing traditional security controls and governance frameworks.

> Shadow AI is already in your software lifecycle, The real question is—can you govern it before it governs you?”
>
> *Vladimir Tyomin, CTO at Commugen*

These tools operate inside integrated development environments (IDEs) and browsers, making them difficult to detect and monitor with conventional enterprise systems. The result is a new category of risk that blends data exposure, compliance failure, and insecure code injection with significant consequences for organizations across every industry.

“Shadow AI is already in your software lifecycle,” said Tyomin. “The question isn’t whether

developers are using it — they are. The question is whether you have the governance, visibility, and controls to manage it before it becomes your next breach headline."

Defining "Shadow AI"

Shadow AI refers to the unsanctioned or unmonitored use of AI tools within an organization. It's the AI-era equivalent of "Shadow IT" — but with far less visibility and potentially far greater risk. Developers, analysts, and engineers often adopt AI code assistants without formal approval, logging, or compliance integration.

Common Shadow AI tools include:
-GitHub Copilot
-ChatGPT and OpenAI APIs
-Amazon CodeWhisperer
-Claude, Gemini, and Llama models

Because these tools can process sensitive data in real time, they pose particular risks in regulated industries such as finance, healthcare, and critical infrastructure sectors where data protection, traceability, and compliance are non-negotiable.

The Growing Risk Landscape

Traditional governance, risk, and compliance (GRC) systems were never designed to track or regulate AI usage at the level it now occurs in developer environments. This has created a critical blind spot for security leaders.

Key risks include:
1. Insecure Code Suggestions — AI-generated code may appear correct but introduce subtle vulnerabilities, bugs, or logic flaws.
2. Prompt Injection Attacks — Malicious or manipulated input can alter AI behavior, producing harmful outputs.
3. Compliance Violations — AI tools may inadvertently handle data in ways that breach GDPR, ISO 27001, NIS2, or contractual obligations.
4. Unintentional Data Exposure — Developers may unknowingly share sensitive or regulated code when under tight deadlines.
5. Lack of Audit Trail — Most organizations have no logging of AI prompts or responses, leaving compliance teams without traceability.
6. Unauthorized Code Reviews — Using AI for code review without governance may leak proprietary business logic or intellectual property.

Why Now?

The acceleration of AI adoption in development workflows is not slowing down. Analysts estimate that within the next two years, a majority of enterprise software teams will integrate AI-assisted coding into their daily operations. Without visibility and governance, the cumulative risk to code integrity, data security, and compliance obligations will grow exponentially.

Commugen's AI Risk Management Solution

Commugen has launched a dedicated AI Risk Management platform to address these challenges, purpose-built for CISOs, and compliance leaders.

Core capabilities include:

-AI Tool Mapping— Detect unsanctioned AI tools in developer environments through telemetry, surveys, and integrations.

-AI Risk Scoring— Score and classify AI usage by data type and sensitivity.

-AI Regulatory Mapping — Align AI activity with NIST AI RMF, ISO 27001, ISO/IEC 42001, and the EU AI Act.

-Automated AI Governance — Implement policy-driven controls for usage, logging, and reporting.

-Seamless Integration — Commugen's No-code GRC Platform deploys with real-time dashboards that integrate into existing security software via API.

By embedding governance into the developer workflow rather than attempting to block AI outright, organizations can enable innovation while ensuring security and compliance.

Industry Guidance from Commugen

Commugen advises security leaders to treat generative AI as a critical third-party service, applying the same governance standards used for cloud services, APIs, or other high-impact enterprise tools. That means onboarding, monitoring, and enforcing controls from day one.

"The organizations that win in the AI era will be those that establish visibility and guardrails early," Tyomin noted. "Shadow AI can be turned from a liability into a competitive advantage, but only with proactive governance."

About Commugen

Commugen helps organizations transform complex cybersecurity and governance requirements into automated, manageable processes. Their AI powered solutions empower CISOs and compliance leaders to manage risk proactively, integrate security into everyday workflows, and drive innovation without compromising compliance.

For more information, visit www.commugen.com.

Sarah Shetrit
Commugen
email us here
Visit us on social media:
LinkedIn
