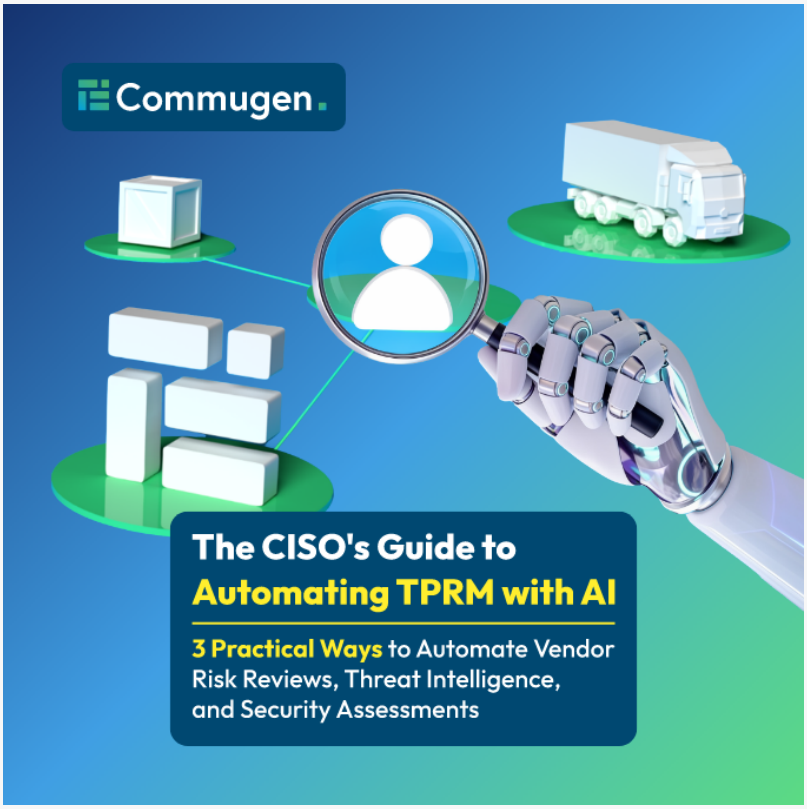
Commugen Launches AI Agents to Automate Third-Party Risk Management (TPRM)

New Commugen AI agents automate vendor reviews, cyber threat intelligence, and vulnerability scanning to help organizations scale Third-Party Risk Management.



LONDON, UNITED KINGDOM, July 7, 2026 /EINPresswire.com/ -- Commugen today announced the launch of three new AI agents purpose-built for Third-Party Risk Management (TPRM), expanding its Cyber GRC platform with capabilities designed to automate vendor security assessments, cyber threat intelligence, and external vulnerability scanning.
The new AI agents help organizations reduce the manual effort required to evaluate third-party cyber risk while improving consistency, visibility, and scalability across vendor risk management programs.

The announcement reflects a growing shift across the cybersecurity industry as organizations increasingly adopt artificial intelligence to strengthen Vendor Risk Management (VRM), Third-Party Risk Management, supplier due diligence, and Cyber GRC operations.
Modern organizations depend on an increasingly complex ecosystem of vendors, suppliers, cloud providers, managed service providers, software vendors, contractors, and business partners.
Every new supplier creates business value.
Every new supplier also introduces cyber risk.

As digital transformation accelerates, organizations now rely on hundreds or even thousands of third parties to operate critical business functions. These vendors often receive access to sensitive information, business applications, production environments, customer data, financial

systems, and operational technology.

This interconnected environment has made Third-Party Risk Management one of the fastest-growing priorities for CISOs and Cyber GRC leaders.
At the same time, cybercriminals increasingly target suppliers as an indirect path into larger organizations. Several of the most significant cyber incidents in recent years have demonstrated that a single compromised vendor can affect hundreds or thousands of downstream organizations.
As supply chain attacks continue to increase, organizations are placing greater emphasis on Vendor Risk Management, third-party cyber risk assessments, supplier due diligence, continuous vendor monitoring, and external security validation.
Regulatory requirements are evolving as well.

Frameworks including NIS2, DORA, ISO 27001, SOC 2, NIST CSF, PCI DSS, and industry-specific regulations increasingly require organizations to demonstrate effective oversight of third-party vendors and supply chain security.
As a result, Vendor Risk Management is no longer viewed solely as a compliance activity.
It has become a core component of cyber resilience.

Although Third-Party Risk Management has become more important than ever, many organizations continue to rely on highly manual processes.
Vendor assessments frequently begin with lengthy security questionnaires that contain hundreds of questions covering governance, identity management, endpoint protection, encryption, vulnerability management, disaster recovery, business continuity, compliance, incident response, and security awareness.
Security teams must then review every response, validate supporting evidence, confirm certifications, identify inconsistencies, verify company information, assess technical controls, and determine whether the supplier meets internal security requirements.
This work is often performed manually.

Analysts compare documents, search for missing evidence, review certifications, research suppliers online, and compile findings into reports for procurement teams, compliance teams, legal departments, auditors, and executive leadership.
As organizations onboard additional suppliers, this process becomes increasingly difficult to maintain.
Vendor assessments take longer.

Security teams spend more time reviewing paperwork than evaluating cyber risk.
Inconsistent review methodologies can lead to different conclusions for similar vendors.
Important findings may be overlooked.
Vendor onboarding slows down.
Business stakeholders become frustrated.
At the same time, third-party risk continues to change long after onboarding is complete.

New vulnerabilities are discovered.
Suppliers experience cyber incidents.
Certificates expire.
Infrastructure changes.
Threat actors evolve.
Point-in-time assessments quickly become outdated.

According to Commugen, these challenges are driving increased demand for AI-powered Third-Party Risk Management platforms that automate repetitive work while giving security professionals better visibility into vendor cyber risk.
Artificial intelligence is rapidly becoming one of the most important technologies in Cyber GRC. However, Commugen believes organizations gain the greatest value when AI is embedded directly into existing security workflows rather than used as a standalone chatbot.

Instead of asking security teams to write prompts or manually analyze large amounts of information, specialized AI agents can perform dedicated Cyber GRC tasks automatically.
Each agent is responsible for a specific workflow.
Each produces explainable results.
Each operates within established governance processes.
This approach enables organizations to accelerate execution without sacrificing transparency or accountability.
Commugen's latest release follows this philosophy.
The company has introduced three specialized AI agents that automate some of the most time-consuming activities within Third-Party Risk Management.

AI Evidence Analysis

The first new capability is Commugen's AI Evidence Analysis agent.
Vendor questionnaires remain one of the most resource-intensive activities in Vendor Risk Management.
Organizations routinely review supplier questionnaires alongside ISO 27001 certificates, SOC reports, penetration test summaries, policies, security documentation, business continuity plans, and other supporting evidence.
Reviewing this material manually requires significant effort.
The AI Evidence Analysis agent automates this review process.
It analyzes completed questionnaires, validates supporting evidence, detects inconsistencies, identifies expired certifications, flags missing documentation, recognizes weak responses, and explains why each issue affects vendor risk.
Rather than simply identifying missing information, the AI maps findings back to organizational controls and provides context that helps analysts understand the significance of every observation.
The result is a faster, more consistent, and more scalable vendor review process.
Organizations can assess more vendors while maintaining a standardized evaluation

methodology across every assessment.
According to Commugen, customers using AI Evidence Analysis can reduce evidence review time by up to 70 percent.

AI Cyber Threat Intelligence

Questionnaires provide valuable information.
However, they only reflect information vendors choose to disclose.
They cannot reveal every publicly documented cyber incident, ransomware attack, breach disclosure, exposed credential, or external security issue.
Security analysts often spend hours researching suppliers using search engines, public reports, security blogs, breach databases, and threat intelligence sources.
Commugen's AI Cyber Threat Intelligence agent automates this work.
Users simply enter a vendor name.
The AI agent conducts extensive OSINT-based research across publicly available sources to identify historical cyber incidents, ransomware activity, documented vulnerabilities, exposed credentials, security advisories, breach reports, and other indicators relevant to supplier cyber risk.
The agent validates supplier identity, analyzes the available evidence, and generates a comprehensive intelligence report complete with supporting references and an overall vendor cyber risk score.
This enables organizations to strengthen vendor due diligence while dramatically reducing manual research.
Instead of collecting information from numerous websites, security teams receive a consolidated intelligence report that supports faster and more informed risk decisions.

AI External Vulnerability Scanning

A supplier may complete a questionnaire successfully and report no known cyber incidents.
That does not necessarily mean the organization's external security posture is strong.
Internet-facing systems change continuously.
New vulnerabilities are disclosed every day.
External assets may expose unnecessary services or outdated software.
Commugen's AI External Vulnerability Scanning agent provides an additional layer of validation.
Users enter a vendor's public domain.
The AI agent automatically evaluates the supplier's external attack surface to identify internet-facing assets, exposed services, known vulnerabilities (CVEs), outdated technologies, SSL/TLS weaknesses, and security misconfigurations.
The findings are organized into a prioritized report that includes an overall vendor security risk score.
This allows organizations to supplement questionnaires with objective technical validation and gain continuous visibility into third-party cyber exposure.

Building AI Agents for Cyber GRC

According to Commugen, these new capabilities represent part of a broader strategy to build specialized AI agents across the Cyber GRC lifecycle.
Rather than developing a single general-purpose assistant, the company is creating AI agents that automate individual Cyber GRC workflows.
Existing AI capabilities within the Commugen platform include AI Policy Generation, AI Mitigation Planning, AI Task Generation, AI GRC Assistant, and AI Evidence Analysis.
Each capability is designed to reduce repetitive work while preserving human oversight, explainability, and auditability.
The objective is not to replace security professionals.
The objective is to help Cyber GRC teams spend less time on administrative work and more time evaluating cyber risk, strengthening governance, improving compliance, and supporting better business decisions.
Commugen states that its AI capabilities operate through secure infrastructure and that customer information is never used to train AI models. Organizations can also deploy AI using private infrastructure when required by internal security or regulatory requirements.

The Future of AI-Powered Third-Party Risk Management

Commugen believes Third-Party Risk Management will continue evolving beyond periodic questionnaires toward continuous, AI-assisted vendor monitoring.
Organizations increasingly require real-time visibility into supplier cyber posture rather than annual or quarterly assessments.
As vendor ecosystems continue to expand, security teams will require technologies capable of reviewing evidence, monitoring external attack surfaces, collecting cyber threat intelligence, identifying emerging risks, and supporting vendor risk decisions at enterprise scale.
Artificial intelligence is expected to play an increasingly important role in achieving these objectives.
By embedding specialized AI agents directly into Cyber GRC workflows, organizations can improve consistency, accelerate assessments, reduce manual effort, and gain greater visibility into third-party cyber risk without increasing headcount.

New Educational Guide Released

Alongside the announcement, Commugen has released a new educational resource titled "The CISO's Guide to Automating TPRM with AI."
The guide explores practical applications of AI within Third-Party Risk Management and demonstrates how organizations can automate vendor evidence reviews, AI-powered cyber threat intelligence, and external vulnerability scanning using specialized Cyber GRC AI agents.
The guide is intended for CISOs, Vendor Risk Managers, Third-Party Risk Management teams, Cyber GRC professionals, security leaders, compliance managers, procurement teams, and organizations seeking practical ways to modernize vendor risk management through artificial

intelligence.

About Commugen

Commugen is a Cyber GRC platform that helps organizations automate cybersecurity governance, risk management, compliance, Third-Party Risk Management, Vendor Risk Management, Compliance management, vulnerability management, mitigation planning, cyber risk operations.
Through a no-code automation platform, advanced analytics, API integrations, and a growing portfolio of specialized AI agents, Commugen enables organizations to reduce manual effort, improve consistency, strengthen cyber resilience, accelerate Third-Party Risk Management, and modernize Cyber GRC programs at enterprise scale.

Adam Babayoff
Commugen
+ +44 20 4591 9206
email us here
Visit us on social media:
LinkedIn