EINPRESSWIRE

CIS, Astrix, and Cequence Unite to Deliver Actionable Guidance for Securing AI Environments

Partnership combines standards, agentic AI enablement, and security controls to help enterprises innovate responsibly with AI

EAST GREENBUSH, NY, UNITED STATES, December 3, 2025 /EINPresswire.com/ -- The Center for Internet Security, Inc. (CIS®), Astrix Security, and Cequence Security today announced a strategic partnership to develop new cybersecurity guidance tailored to the unique risks of artificial intelligence (AI) and agentic systems.

This collaborative initiative builds on the globally-recognized CIS Critical Security Controls® (CIS Controls®), extending its principles into AI environments where autonomous decision‑making, tool and API access, and automated threats introduce new challenges. The intent of the partnership includes initially developing two CIS Controls companion guides: one for AI Agent Environments , which will focus on securing the agent system lifecycle; the other for Model Context Protocol (MCP) environments.

MCP environments introduce unique risks, including credential exposure, ungoverned local execution, unapproved third‑party connections, and uncontrolled data flows between models and tools. Together, these guides will provide targeted safeguards for organizations operating in environments where MCP agents, tools, and registries interact dynamically with enterprise systems.

“AI presents both tremendous opportunities and significant risks,” said Curtis Dukes, Executive Vice President and General Manager of Security Best Practices at CIS. “By partnering with Astrix and Cequence, we are ensuring that organizations have the tools they need to adopt AI responsibly and securely.”

Astrix's contribution centers on securing AI agents, MCP servers, and the Non-Human Identities (NHIs), such as API keys, service accounts, and OAuth tokens, that link them to critical systems.

“AI agents and the non-human identities that power them bring great potential but also new risks,” said Jonathan Sander, Field CTO of Astrix Security. “Our focus is helping enterprises discover, secure, and deploy AI agents responsibly, with the confidence to scale. Through this partnership, we’re providing clear, practical guidance to keep AI ecosystems safe so organizations can innovate with confidence.”

Cequence brings years of enterprise application and API security experience to agentic AI enablement and security.

“As organizations embrace agentic AI, trust hinges on visibility, governance, and control over what those agents can see and do to your applications and data,” said Ameya Talwalkar, CEO of Cequence Security. “Security is strongest through collaboration, and this partnership gives organizations clear guidance to adopt AI safely and securely.”

How the Partnership Supports Organizations

- Extends trusted cybersecurity frameworks into AI environments, addressing risks from autonomous systems and integrations.
- Delivers clear, prioritized safeguards that guide enterprises toward secure and responsible AI adoption.
- Combines expertise across standards, API security, and application defense to provide comprehensive protection.

The new guidance is scheduled for release in early 2026, accompanied by workshops, webinars, and supporting resources delivered jointly by CIS, Astrix, and Cequence. Together, the organizations aim to help enterprises translate recommendations into practice while building a stronger foundation of trust, transparency, and resilience across the AI ecosystem. By working from a shared framework, enterprises, vendors, and security leaders can align on a common language for securing AI environments.

###

About CIS

The Center for Internet Security, Inc. (CIS) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks® guidelines, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®) organization, the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®) organization, which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit cisecurity.org or follow us on X: @CISecurity.

About Astrix Security
Astrix secures the full lifecycle of AI agents and the Non-Human Identities (NHIs) that power them, extending traditional IAM to govern the modern AI attack surface. While agents and other NHIs outnumber humans 100:1, they remain under the radar, creating the biggest blind spot in our identity perimeter. Astrix provides a unified solution for continuous discovery of all AI agents and NHIs, security and remediation of excessive privileges, protection against real-time threats, and responsible adoption of new agents with 'secure by design' guardrails like agentic just-in-time access. This enables enterprises to adopt AI responsibly while accelerating productivity. Astrix is trusted by leading organizations including Workday, NetApp, Priceline, Figma, HubSpot, Workato, and many more. To learn more, visit https://astrix.security/.

About Cequence Security
Cequence is a pioneer in API security and bot management, making the applications and APIs that organizations depend on AI-ready while protecting them from attacks, business logic abuse, and fraud. Our unique solutions unlock the promise of agentic AI productivity while providing real-time security against increasingly subtle and sophisticated threats. Cequence delivers value in minutes rather than days or weeks with a highly scalable no-code, no-risk approach. Trusted by the largest and most demanding private and public sector organizations, Cequence protects more than 10 billion daily API interactions and 4 billion user accounts. To learn more, visit www.cequence.ai.

Kelly Wyland
Center for Internet Security
+1 518-256-6978
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.