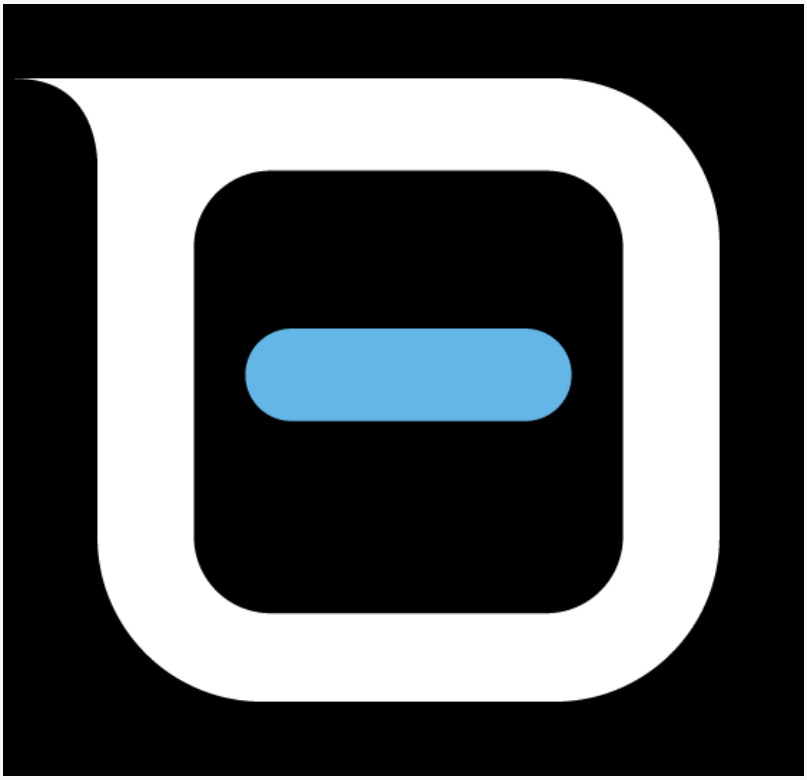
Introducing the Agent Skills Security Index

The Agent Skills Security Index community powered by Tego is a public database that analyzes and maps security risks within AI agent capabilities and workflows.


The Agent Skills Security Index

SAN FRANCISCO, CA, UNITED STATES, March 18, 2026 /EINPresswire.com/ -- A New Database Maps the Security Risks of AI Agent Skills

A new public database has launched to analyze the security risks introduced by AI agent skills, the capabilities that increasingly define how modern AI agents operate. The site available at https://index.tego.security/skills/ presents what appears to be the first dedicated database focused on the security assessment of AI agent skills. The project, called the Agent Skills Security Index, catalogs the capabilities these modules grant to AI systems and evaluates the risks they may introduce into agent-driven workflows.

The Agent Skills Security Index is an initiative of the Agent Skills Security Index community, which aims to provide security researchers and practitioners with a structured way to analyze the emerging attack surface created by AI agent capabilities.
AI skills, sometimes called tools, functions, or plugins, are rapidly becoming the core building blocks of agentic AI systems. They allow language models to retrieve data, perform specialized reasoning tasks, and execute automated workflows.
But these capabilities also introduce a new layer of attack surface that many organizations are only beginning to understand. Research examining large ecosystems of agent skills has already found that more than a quarter contain at least one security vulnerability, including prompt injection vectors, privilege escalation opportunities, and data-exfiltration risks.

The new database aims to make this emerging attack surface visible.
Each skill entry includes a structured security analysis designed to help practitioners understand how a capability might be abused inside real agent deployments. The assessment process uses a

> The Agent Skills Security Index provides a structured way to analyze the emerging attack surface created by AI agent capabilities, helping teams understand how behavior translates into risk."
>
> *Agent Skills Security Index community powered by tego.ai*

multi-dimensional security methodology combining automated scanning, specialized AI models trained to analyze agent behavior, and manual security review.

Rather than simply flagging potentially dangerous code patterns, the analysis follows a practical philosophy: instructions and behaviors are evaluated within the context of the skill's intended purpose. This allows the review process to distinguish between normal operational capabilities and behaviors that could realistically be exploited by attackers manipulating an AI agent's reasoning process.
The project reflects a broader shift occurring in AI system security. As AI agents move beyond text generation into task execution and autonomous workflows, the security boundary is increasingly defined by the capabilities those agents can invoke.

In this model, skills effectively become the execution layer of AI systems, capable of:
• influencing agent decision-making
• injecting context into reasoning processes
• triggering automated actions
• exposing data through tool outputs
• interacting with other agents

Security researchers are beginning to recognize that these capabilities introduce attack patterns with few direct parallels in traditional software, including indirect prompt injection through retrieved content and confused-deputy attacks caused by agent tool invocation.
By cataloging and analyzing these capabilities, the Agent Skills Security Index aims to provide security teams with a clearer understanding of how agent behavior translates into real security risk.

The resource is publicly accessible and is expected to expand as the ecosystem of AI agent skills continues to grow.
The initiative is supported by contributors from the AI security community, including researchers working on security technologies for the emerging agentic AI ecosystem and powered by Tego.AI

Dan Benger
Tego AI
email us here
Visit us on social media:
LinkedIn
X

This press release can be viewed online at: https://www.einpresswire.com/article/900284469

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something 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.
© 1995-2026 Newsmatics Inc. All Right Reserved.